HAAGA-HELIA
ammattikorkeakoulu

Sovelluspäivitysten levityksen hallinta

Marko Riihijärvi

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2016

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

16.6.2016

Tekijä(t)
Marko Riihijärvi

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Sovelluspäivitysten levityksen hallinta

Sivu- ja liitesivumäärä
61

Opinnäytetyön otsikko englanniksi
Management of software updates deployment

Opinnäytetyön tarkoituksena on helpottaa muiden kuin Microsoftin sovellusten tietoturvapäivitysten levittämistä SCCM (System Center Configuration Manager) 2012:lla, tätä varten tehdään tuotannon käyttöönottosuunnitelma SCUP (System Center Updates Publisher) 2011 -työkalulle. Työkalu asennetaan ja testataan SCCM 2012 -testiympäristössä mikä on identtinen projektin toimeksi antavan organisaation tuotantoympäristön kanssa.

SCUP 2011 -työkalun avulla voidaan luoda, muokata ja julkaista muiden ohjelmistotoimittajien kuin Microsoftin ohjelmistopäivityksiä WSUS (Windows Server Updates Services) -palvelimelle, mistä ne voidaan hakea ja levittää tietoturvapäivityksinä SCCM 2012:lla. Näin levitettynä päivitykset eivät näy käyttäjille häiritsevinä asennusikkunoina, eivätkä asennukset vaadi pakotettua työaseman uudelleen käynnistämistä.

Teoriaosassa käydään läpi mitä on tieto- ja kyberturvallisuus, minkälaisia kyberuhkia tietojärjestelmiin ja tietoteknisiin ympäristöihin kohdistui vuonna 2015 sekä haettiin kansainvälisestä haavoittuvuustietokannasta käyttöjärjestelmien ja ohjelmistojen ilmoitettuja haavoittuvuuksia eri kriteereillä vuosilta 2011–2015.

Toteutusosassa käydään läpi mitä asetuksia ja muutoksia SCUP 2011 -työkalun asennus vaatii. Opinnäytetyön tuotoksena syntyy testausympäristössä toteutettu suunnitelma SCUP 2011 -työkalun käyttöönottamiseksi. Rajauksena opinnäytetyölle on, että siinä ei käydä läpi SCCM 2012 -operointia.

Asiasanat
Tietoturvallisuus, Kyberturvallisuus, System Center Configuration Manager, System Center Updates Publisher, Tietoturvapäivitykset, Sovelluspäivitykset

HAAGA-HELIA
University of Applied Sciences

Abstract

16.6.2016

Author(s)
Marko Riihijärvi

Degree programme
Business Information Technology

Report/thesis title
Management of software updates deployment

Number of pages and appendix pages
61

The purpose of this thesis was to make it easier to deploy 3rd party software vendor's software updates with SCCM 2012. For this a deployment plan was completed for production environment for SCUP 2011 tool. The tool was installed and tested in the SCCM 2012 testing environment, which is similar to the organisation´s production environment.

The tool will provide an ability to create, modify and publish software updates from software vendors other than Microsoft to WSUS server, from where updates can be downloaded and deployed as security updates with SCCM 2012. Updates deployed this way don´t show as disturbing pop-up windows to users and installation doesn´t need forced computer restart.

The theory part goes through what is information security and cybersecurity and what kinds of cyber threats were directed against information systems in the year 2015. Also published vulnerabilities of software and operating systems were searched with various criteria from National Vulnerability Database from years 2011–2015.

The empirical part goes through what kinds of settings and changes the installation of SCUP 2011 tool needs. The product of this thesis is the deployment plan for SCUP 2011 tool which was completed in the testing environment. The operating of SCCM 2012 is left outside the scope of the study.

Keywords
Information security, Cybersecurity, System Center Configuration Manager, System Center Updates Publisher, Security updates, Software updates

Sisällys

Sanasto

SCUP (System Center Updates Publisher) on työkalu, millä voidaan julkaista muiden sovellustoimittajien kuin Microsoftin sovelluspäivityksiä päivityspalvelimelle.

SCCM (System Center Configuration Manager) on järjestelmä millä voidaan levittää ohjelmistoja ja niiden päivityksiä sekä ylläpitää laitteistoinventaariota organisaation it-ympäristössä.

AD (Active Directory) on toimialueen käyttäjätietokanta ja hakemistopalvelu.

AD CS (Active Directory Certificate Services) on Windowsin palvelu, millä luodaan ja hallitaan julkisen avaimen infrastruktuurin varmenteita.

WSUS (Windows Server Update Services) on Windowsin palvelu, millä voidaan hallita ja levittää Microsoftin sovelluksien päivityksiä.

GPO (Group Policy Object) on ryhmäkäytäntöobjekti, joilla hallitaan toimialueen käyttäjiä ja tietokoneita.

MMC (Microsoft Management Console) on hallintakonsoli, jonka näkymään voi lisätä erilaisia hallintaikkunoita.

CAS (Central Administration Site) on SCCM:n palvelin, mistä ympäristön hallinta ja asetusmuutokset tehdään keskitetysti.

CVSS (Common Vulnerability Scoring System) on avoin viitekehys haavoittuvuuksien pisteytykselle.

NVD (National Vulnerability Database) on yhdysvaltalaisen NIST-viraston ylläpitämä tietokanta sovellusten haavoittuvuuksista.

1 Johdanto

Tietomurroista it-infrastruktuureihin ja käyttäjien tietojen, kuten osoite- ja luottokorttitietojen varastamisesta on viime vuosina tullut yleinen aihe uutisten otsikoissa. Opinnäytetyön teon aikaan olin vastuussa työskentelemäni organisaation päätelaitteiden tietoturvapäivitysten levityksen hallinnasta. Työn kuvani ja koko ajan uhkaavampien tietoturvauhkien takia aloitin SCUP 2011 -työkalun käyttöönottoprojektin suunnittelun.

Työn kohteena on tehdä SCUP 2011 -työkalun käyttöönottosuunnitelma. Kyseinen järjestelmä integroituu SCCM 2012 -järjestelmään ja työssä tehdään SCUP 2011 -työkalun käyttöönottosuunnitelma tuotantoympäristöön. Järjestelmät liittyvät työasemien hallintaan ja sovellusten automatisoituihin massa-asennuksiin. Työn tilanneen organisaation työasemaympäristö on erittäin suuri ja monissa toimipisteissä työskennellään ympärivuorokautisesti, joten sovelluspäivitysten ajoituksen hallinta on monimutkaista. SCUP 2011 -työkalu tulee helpottamaan sovelluspäivitysten jakelua muiden valmistajien kuin Microsoftin sovelluksiin.

Työasemaympäristön ollessa suuri ja kriittinen, pitää sovellusten käyttökatkojen määrät saada minimoitua. Yleensä sovellustoimittajien tuotteet päivittyvät kerran kuussa, jolloin päivityksiä asennetaan koko ajan. Jos päivityksiä ei asenneta tulevat vastaan tietoturvaongelmat, koska päivitykset ovat yleensä haavoittuvuuksia korjaavia tietoturvapäivityksiä. Sovelluksia ei voida päivittää sattumanvaraisesti, koska niillä saattaa olla vaikutuksia kriittisiin järjestelmiin, joten kaikki päivitykset pitää testata tuotantoympäristössä huolellisesti sovellustestaajien toimesta.

Opinnäytetyön tavoitteena on saada käyttöönottosuunnitelma SCUP 2011 -työkalulle. Työ tehdään ja testataan SCCM 2012 -testiympäristössä, mikä on identtinen organisaation tuotannon SCCM 2012 -järjestelmäympäristön kanssa. SCUP 2011 -työkalun käyttöönotto helpottaa sovelluspäivitysprosessin ohjausta ja hallintaa. Rajauksena opinnäytetyölle on, että siinä ei käydä läpi SCCM 2012 -järjestelmän operointia.

Tässä työssä vastataan seuraaviin tutkimusongelmakysymyksiin:

- Mitä on tieto- ja kyberturvallisuus?
- Mikä on SCUP 2011?
- Miten SCUP 2011 toimii?
- Mitä hyötyä SCUP 2011 -työkalun käytöstä on?
- Miten SCUP 2011 -työkalu otetaan käyttöön?

2 Tietoturvallisuus

Yrityksen tietoturvallisuus noudattaa ohjeistavia toimenpiteitä, mitkä on määritetty tietoturvallisuuden kehittämissuunnitelmassa. Näillä korjataan havaitut puutteet, jotka nousevat esille tietoturvallisuuden arvioinneissa. (VAHTI 08 2008, 119.) Tietoturvallisuus on järjestelyitä, joilla pyritään turvaamaan tiedon käytettävyys, eheys ja luottamuksellisuus laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta (VAHTI 03 2007, 14).

Käytettävyydellä tarkoitetaan, että tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla siihen oikeutetuille (VAHTI 08 2008, 56). Eheydellä tarkoitetaan, että tietoa tai viestiä ei ole muutettu valtuudettomasti, ja että muutokset ovat luettavissa kirjausketjusta (VAHTI 08 2008, 27). Luottamuksellisuudella tarkoitetaan, että ainoastaan ne henkilöt joilla on oikeudet pääsevät käyttämään tietoa (Järvinen 2002, 22).

2.1 Kyberturvallisuus

Puhuttaessa kyberturvallisuudesta on tärkeää keskittyä sanaparin toiseen sanaan eli turvallisuuteen. Turvallisuus voidaan kuvailla tavoitetilaksi, minkä yritämme saavuttaa erilaisin turvallisuutta korottavin toiminnoin. Halutun turvallisuuden tason ja sen ylläpitämisen estää uhat. Turvallisuuden arvioinnit ja parantamiset alkavat uhkien arvioinnilla. Uhka on tekijä joka edustaa vaaraa, vahinkoa ja turvattomuutta. Määrittelemällä riskit ymmärrämme paremmin etsimämme turvallisuuden tason, arvioimme eri muuttujia mitkä uhkaavat sitä ja se myös lisää ymmärrystämme mitä toimenpiteitä tarvitaan saavuttaaksemme sen. (Limnéll, Majewski, Salminen & Samani 2015, 33–34.)

Luottamuksella on hyvin keskeinen rooli kyberturvallisuudessa. Kyberympäristö voidaan ajatella turvalliseksi, kun voimme luottaa sen toimivuuteen. (Limnéll ym. 2015, 39.)

Kybermaailman negatiivinen puoli, joka pääosin koostuu uhkista ja eri haavoittuvuuksista järjestelmissä joihin luotamme. Kyberturvallisuudella suojaudumme negatiivisilta tekijöiltä, ennaltaehkäisemme ja puolustaudumme sekä minimoimme niiden vaikutuksia. Tämä tekee kyberturvallisuudesta voimakkaasti uhkiin painottuvan. Kolme käsitettä helpottaa selviytymisestä bittimaailman negatiivisesta puolesta: uhkat, riskit ja haavoittuvuudet. Uhkat, riskit ja haavoittuvuudet eivät ole yksi ja sama asia, vaikka kaikilla kolmella on samanlaisia ominaisuuksia, kuten niiden suhteellisuudet ja rajoittuneisuudet resursseja, aikaa, potentiaalia ja vahinkoja vastaan. Kuitenkin suurimmaksi osaksi aikaa niiden ominaisuudet, toi-

minnot ja vasta-toiminnot ovat erilaisia. Uhkat, riskit ja haavoittuvuudet ovat aina toimija ja tilannekohtaisia. (Limnéll ym. 2015, 103.)

2.1.1 Uhka, riski ja haavoittuvuus

Praxiomin (2014) mukaan uhka on potentiaalinen tapahtuma. Kun uhkasta tulee todellinen tapahtuma, voi se aiheuttaa ei-toivotun tapauksen. Se on ei-toivottu, koska tapaus voi aiheuttaa vahinkoa organisaatiolle tai järjestelmälle.

Tietoturvariski monesti kuvaillaan kahdella tekijällä, todennäköisyydellä ja seurauksella. Siinä kysytään kaksi peruskysymystä, millä todennäköisyydellä kyseinen tietoturva tapahtuma tapahtuu tulevaisuudessa? Ja mitä seuraamuksia tämä tapahtuma tuottaa tai mikä vaikutus sillä on, jos se todella tapahtuu? (Praxiom, 2014.)

Toisin kuin uhkaa, riskiä ei voida torjua koska se esiintyy kaikessa toiminnassa, myös bittimaailmassa. Riski ei myöskään ole ongelma, koska ongelmat ovat seurauksia jostain jo tapahtuneista asioista. Riski on normaalitila mikä huomioi mahdollisen uhkan ja vertailee sen todennäköistä esiintyvyyttä ja mahdollista vaikutusta. Riski ei ole selvästi hyvä tai huono asia, vaan riski ennemminkin muuttuu ajan kuluessa. Sen sijaan että jättäisimme ne huomioimatta, riskejä voidaan tarkastella eri tavoilla, esimerkiksi välttelemällä, hyväksymällä, vähentämällä, tai jopa siirtämällä niitä. (Limnéll ym. 2015, 105.)

Tietotekniikassa haavoittuvuus viittaa heikkouteen, mikä mahdollistaa hyökkääjän heikentää kohdejärjestelmän tiedon luotettavuutta ja/tai käytettävyyttä. Haavoittuvuus syntyy, kun järjestelmässä on vika tai heikkous, jota hyökkääjä osaa hyödyntää. Mitä paremmat ovat järjestelmän sietokyky- ja palautumisominaisuudet, sitä vähemmän haavoittuvampi se on uhkan edessä. Tämän päivän suurimmat haavoittuvuudet ovat tietojärjestelmissä ja kriittisissä tietoinfrastruktuureissa. (Limnéll ym. 2015, 108.)

2.1.2 Kyberuhat vuonna 2015

ENISA on julkaissut raportin missä se käy läpi vuoden 2015 vakavimmat kyberuhat. Erilaisia uhkia on 15 ja viisi vakavinta niistä on samat kuin vuonna 2014. (ENISA 2016, 7.)

ENISAn (2016, 18–29) raportin mukaan viisi vakavinta kyberuhkaa aikavälillä marraskuu 2014 - marraskuu 2015 olivat haittaohjelmat, hyökkäykset internetissä, hyökkäykset verkkosovelluksiin, bottiverkot ja palvelunestohyökkäykset:

Haittaohjelmat: vuonna 2015 monimutkaiset haittaohjelmat näyttivät potentiaalinsa. Esimerkiksi Equation-niminen rikollisryhmä käyttää laitteisto-ohjaimen uudelleenohjelmointia asentaakseen haittaohjelmia kovalevyn laitteisto-ohjaimeen. Tämmöinen haittaohjelma on haastava tunnistaa ja puhdistaa, koska se on asennettu laiteohjelmistoon se kestää niin kovalevyn alustuksen kuin käyttöjärjestelmän uudelleen asennuksen. Laitteistot jotka ovat saastuneet tällä tavoin pitää mahdollisesti vaihtaa kokonaan. Mobiililaitteiden haittaohjelma löydökset eivät saavuttaneet odotettua tasoa, mutta on se silti vakava huolenaihe. Toiseen vuosineljännekseen mennessä mobiililaitteiden haittaohjelmanäytteitä oli yhteensä noin kahdeksan miljoonaa. (ENISA 2016, 19–21.)

Vanhat saastuttamistekniikat nousivat suuntauksena, esimerkiksi melkein 20 vuotta sitten käyttöönotettu Microsoft Office -asiakirjojen mukana haittaohjelmia lataavat Visual Basic -makrovirukset. Yli 7 vuotta vanha Conficker-mato pitää kärkisijaa tietokoneiden saastuneisuus statistiikoissa (37 % kaikista saastuneista). Toiseksi yleisin haittaohjelma on Kilim-mato, mikä perustuu sosiaalisenmedian väärinkäyttöön, tämä todistaa, että sosiaalinen media on noussut pääpaikaksi käyttäjien huijattavaksi houkuttelemiseksi. Erilaisia haittaohjelmia on yhteensä jo yli kaksi miljardia ja uusia haittaohjelmanäytteitä löydetään noin miljoona päivittäin. Kyberrikolliset myös julkaisevat työkaluja joilla teknisesti heikompitaitoiset pystyvät luomaan omia muunnelmiansa haittaohjelmista. (ENISA 2016, 19–21.)

Hyökkäykset internetissä: kyberrikolliset etsivät internetissä hyökkäyksen kohteita, kohteina ovat niin palvelimet kuin käyttäjien päätelaitteet. Hyökkäykset koostuvat haitallisista verkko-osoitteista ja -sivuista, haittaohjelmien automaattisista latauksista verkkosivuilta, verkossa olevista takaporteista ja selaimista löytyvistä tietoturva-aukoista. Haitallisia verkko-osoitteita internetistä löytyy jo satoja miljoonia ja tämä hyökkäystyyppi jatkaa näistä käytetyimpänä. Näistä osoitteista joko jaetaan haittaohjelmia tai ne ohjaavat sivuille, jotka jakavat haittaohjelmia käyttäjien päätelaitteille. (ENISA 2016, 22–23.)

Viestintävirastot löytävät 58 tuhatta haitallista verkko-osoitetta päivittäin, se tekee noin 20 miljoonaa osoitetta vuosittain. Sen tiedon perusteella että 90 % näistä osoitteista muuttuu päivittäin tai tunneittain, tekee kokonaisuudessaan muutaman sataa miljoonaa haitallista verkko-osoitetta. Viisi käytetyintä hyväksikäyttö palvelukategoriaa ovat teknologia, sisällönisännöinti, bloggaus, liiketoiminta ja yksityisyyttä tarjoavat palvelut. Tavallisin uhka on selainten tietoturva-aukkojen hyväksikäyttö, seuraavina tulevat virukset ja tietojenkalastelu. Haitalliset verkko-osoitteet ovat toisena internetin kahdenkymmenen haitallisimpien asioiden listalla. (ENISA 2016, 22–23.)

Hyökkäykset verkkosovelluksiin: Sovellukset ovat nykyään kasvavassa määrin avoinna verkkoon päin tai ne käyttävät verkkoresursseja, siksi hyökkäyksistä verkkosovelluksiin on tullut vakava hyökkäysreitti. Hyökkäystaktiikat eroavat verkkosovelluksien ja mobiilisovelluksien välillä siinä, että hyökkäykset mobiilisovelluksiin perustuu ohjelmoinnin laatuun ja hyökkäykset verkkosovelluksiin hyväksikäyttää usein ohjelmaa ajavaa käyttöympäristöä. Yhdysvallat melkein monopolisoi tilastoja verkkosovelluksien hyökkäyskohteena, houkutellen noin 80 % hyökkäyksistä maailmanlaajuisesti. (ENISA 2016, 24–25.)

Suurimmat haavoittuvuuksien korjausmäärät saavutetaan, kun mukautuvuus on eteenpäin vievä tekijä, kun taas riskeihin orientoituvan asenteen johdosta tehtävä haavoittuvuuksienkorjaus tuottaa pienimmät korjaus määrät. Verkkosovelluksiin kohdistuvat hyökkäykset ovat voimakkaasti kehittyviä sekä monipuolisia, niillä on myös potentiaalia nousta ylemmäs listalla kyberuhkien kärkeen. Maat joilla on tietynlaisia varallisuuksia, tulisi odottaa hyökkäyksiä rahoitusalan sovelluksiin. (ENISA 2016, 24–25.)

Bottiverkot: Bottiverkot ovat yksi tärkeimmistä infrastruktuureista, kun tietyntyyppisiä kyberuhkia levitetään. Bottiverkot koostuvat ohjaus- ja valvontapalvelimista sekä saastuneista tietokoneista, joita yleensä on muutamia satoja tuhansia mukana hyökkäyksessä. Bottiverkkojen ollessa tärkeitä kyberrikollisille, myös rikollisuutta vastaan taistelevat tahot kohdistavat kiinnostuksensa niihin. Viranomaiset ovat operaatioidensa avulla saaneet alas ajettua bottiverkkoja maailmanlaajuisesti. Samanaikaisesti kyberrikolliset jatkavat erilaisten metodien ja tekniikoiden kehittämistä saadakseen vaikeammin löydettäviä bottiverkkoja. (ENISA 2016, 25–27.)

Bottiverkon eliniän keskiarvo on 38 päivää ja niiden koon keskiarvo on noin 1700 saastunutta palvelinta. Vuonna 2015 tunnistettiin noin 600–1000 ohjaus- ja valvontapalvelinta, joista jokainen hallitsi paria sataa tuhatta saastunutta tietokonetta. On väitetty, että bottiverkon operaattorit ovat alkaneet suosia virtuaalikoneita ohjaus- ja valvontapalvelin infrastruktuureissaan. Tällä tavoin he pääsevät hyödyntämään virtuaalialustan teknisiä etuja, kuten suorituskykyä, tehokasta hallintaa ja skaalautuvuutta, alentunutta kiinni jäämisen riskiä ja pilviteknologian vakautta. (ENISA 2016, 25–27.)

Palvelunestohyökkäykset: vuonna 2015 palvelunestohyökkäykset olivat edelleen tärkeä työkalu kyberrikollisille. Hyökkäyksien kehityssuunta oli selkeästi se, että niiden lukumäärä kasvoi, lukumäärän kasvu toi lisää hyökkäyksiä mutta vähemmällä kaistanleveydellä kuin edellisenä vuonna, myös hyökkäyksien kesto kasvoi. Toinen muutos hyökkäysprofiilissa liittyy käytettyyn infrastruktuuriin, tehokkaiden palvelin bottiverkkojen sijasta hyökkäyksis-

sä käytettiin huokeampia laitteita kuten kotireitittimiä, sulautettuja järjestelmiä sekä muita internetiin kytkettyjä laitteita. Rikolliset käyttivät myös uutta rahastuskeinoa, yrittäessään rahastaa hyökkäyksen kohteita palvelunestohyökkäyksen lopettamisella.
(ENISA 2016, 28–29.)

Verrattuna edelliseen vuoteen palvelunestohyökkäyksien kokonaismäärä kasvoi 130 %, hyökkäykset sovelluksiin kasvoi 120 %, hyökkäykset infrastruktuureihin kasvoi 130 % ja kasvu yli 100 gigatavua kaistanleveyttä käyttävissä hyökkäyksissä oli 100 %. Kyberrikollisten markkinat tarjoavat palvelunestohyökkäystä maksullisena palveluna ja kuka vaan pystyy tätä kautta järjestämään tehokkaita palvelunestohyökkäyksiä huokeaan hintaan. Tutkimukset osoittavat, että kaksi kolmasosaa hyökkäyksen uhreista menettivät hetkellisesti pääsyn kriittiseen tietoon, kolmasosa ei pystynyt tuottamaan ydinliiketoimintaansa ja toinen kolmasosa menetti liiketoimintamahdollisuuksia tai -sopimuksia. (ENISA 2016, 28–29.)

2.2 Haavoittuvuudet ohjelmistoissa

Haavoittuvuudet ovat heikkouksia ohjelmistoissa, jotka voivat mahdollistaa hyökkääjän vaarantaa ohjelmiston eheyttä, käytettävyyttä ja luottamuksellisuutta. Jotkin pahimmat haavoittuvuudet mahdollistavat hyökkääjän suorittaa mielivaltaista koodia saastuneessa järjestelmässä. Haavoittuvuuksien paljastaminen on haavoittuvuuksien olemassaolon paljastamista julkisesti kaikille. Haavoittuvuuksien paljastukset voivat tulla monesta lähteestä kuten ohjelmistojen toimittajilta, tietoturvaohjelmistojen toimittajilta, yksityisiltä tietoturvatutkijoilta sekä jopa haittaohjelmien luojilta. Suurimman osan ajasta haavoittuvuudet ovat luokiteltu monimutkaisuudeltaan mataliksi, mikä tarkoittaa, että niitä voidaan suhteellisen helposti käyttää hyväksi ilman erityisiä pääsyolosuhteita. (Microsoft 2011a, 2–4.)

Haavoittuvuudet ovat koko toimialan laajuinen ongelma. Vuosittain paljastetaan tuhansia haavoittuvuuksia Microsoftin ja muiden ohjelmistovalmistajien ohjelmistoissa, joten tietoturvapäivitysten hallinta on elintärkeää. Hyökkäyssovelluksilla käytetään hyväksi sovellusten haavoittuvuuksia, vielä vuonna 2011 löytyi hyökkäyssovelluksia vuonna 2003 korjattuihin haavoittuvuuksiin. Tämä todistaa, että hyökkääjät yrittävät rutiininomaisesti vuosia löytää hyväksi käytettäviä järjestelmiä, joihin ei ole asennettu haavoittuvuuksia korjaavia tietoturvapäivityksiä. Nopea ja jatkuva tietoturvapäivitysten asennus voisi estää hyökkäysten onnistumisen tuettuihin sovellusversioihin. Eri alustojen tietoturvapäivitysten hallinnasta on tullut keskeinen osa riskienhallintametodologiassa kaikissa internetiin yhteydessä olevissa ympäristöissä. Sovellushaavoittuvuudet ovat tulleet jäädäkseen, ne ovat mukana koko sovellustuotteen elinkaaren läpi, niin ajatuksesta käyttöönottoon sekä siitä eteen-

päin, näin ollen on mahdotonta ennaltaehkäistä kaikkia haavoittuvuuksia. (Microsoft 2011a, 5–7.)

2.2.1 Haavoittuvuuksien luokittelu

Yleinen haavoittuvuuksien luokittelujärjestelmä CVSS (Common Vulnerability Scoring System) tarjoaa keinon tallentaa haavoittuvuuden pääpiirteet ja tuottaa haavoittuvuuden vakavuudelle numeerinen arvo. Numeerinen arvo voidaan muuntaa luokittelevaan tekstimuotoon esim. matala, keskisuuri tai korkea ja täten helpottaa organisaatioita määrittämään ja priorisoimaan haavoittuvuuksien hallintaprosesseja. (FIRST 2015, 5.)

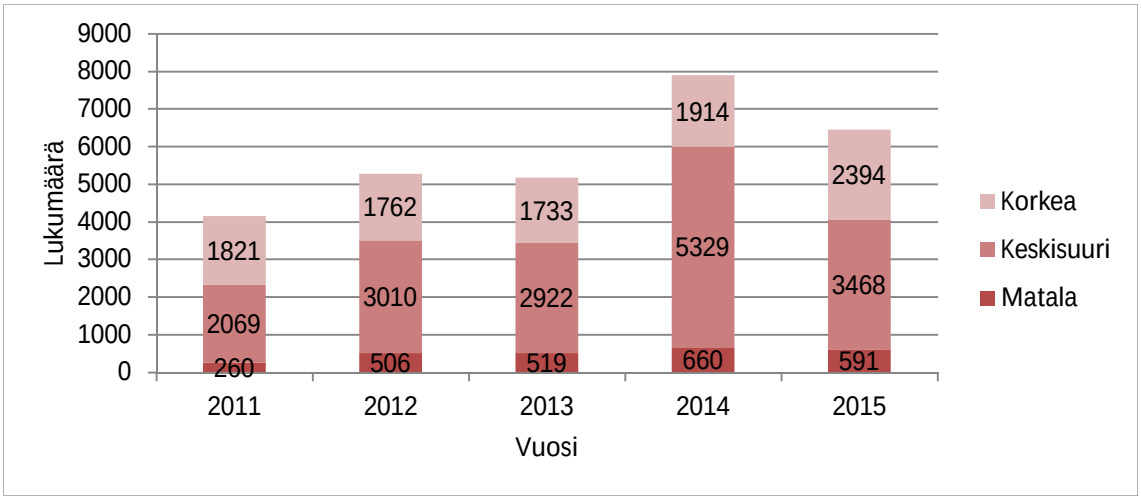
FIRSTin (2015, 5) mukaan yleinen haavoittuvuuksien luokittelujärjestelmä tarjoaa kolme tärkeää hyötyä: standardoidut haavoittuvuusarvot, avoimen viitekehyksen ja priorisoidut riskit.

Yleinen haavoittuvuuksien luokittelujärjestelmä koostuu kolmesta mittaryhmästä, juuri-, aika- ja ympäristötasoista, jokainen näistä sisältää joukon mitta-arvoja. Juuritaso edustaa haavoittuvuuden olennaisia ominaisuuksia, jotka ovat muuttumattomia niin ajallisesti kuin käyttäjäympäristöissäkin. Se sisältää kaksi arvojoukkoa, hyväksikäytettävyys- ja vaikutusarvot. Aikataso edustaa haavoittuvuuden ominaisuuksia, jotka voivat muuttua ajan kuluessa, mutta eivät käyttäjäympäristöissä. Ympäristötaso edustaa haavoittuvuuden ominaisuuksia, jotka ovat yksilöllisiä tietyn käyttäjän ympäristölle. (FIRST 2015, 5–6.)

2.2.2 Tilastoja julkaistuista haavoittuvuuksista

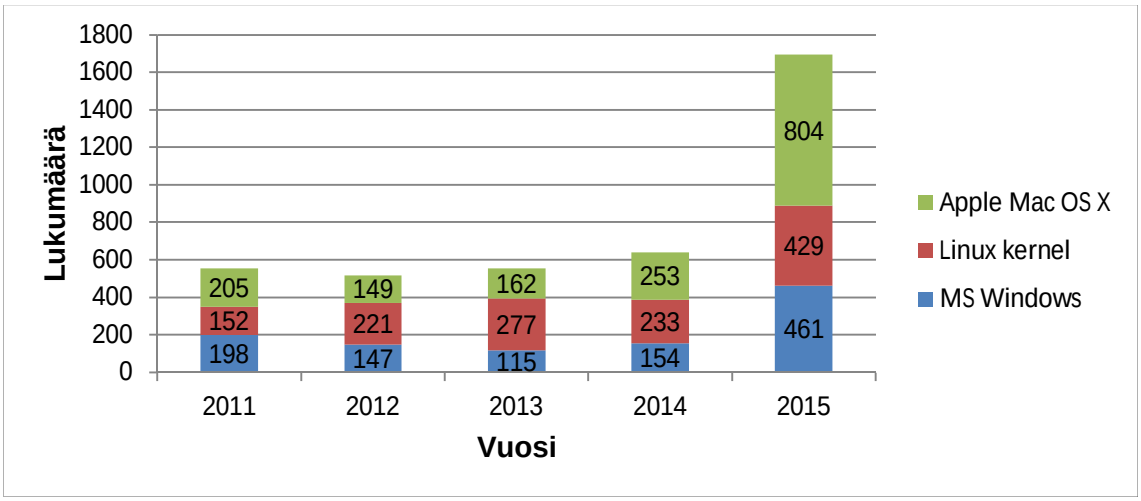
Kansallinen haavoittuvuustietokanta NVD (National Vulnerability Database) on Yhdysvaltain kauppaministeriön alaisen NIST (National Institute of Standards and Technology) -viraston tuote ja sinne kerätään tietoa ohjelmistojen haavoittuvuuksista. (NVD 2016.)

Kuvioon 1 on haettu Kansallisesta haavoittuvuustietokannasta kaikki julkaistut haavoittuvuudet niiden vakavuusluokituksella vuosilta 2011–2015. Kuviossa 1 on vuonna 2014 ollut paljon haavoittuvuuksien löydöksiä, keskisuuria löydöksiä on huomattavan paljon.



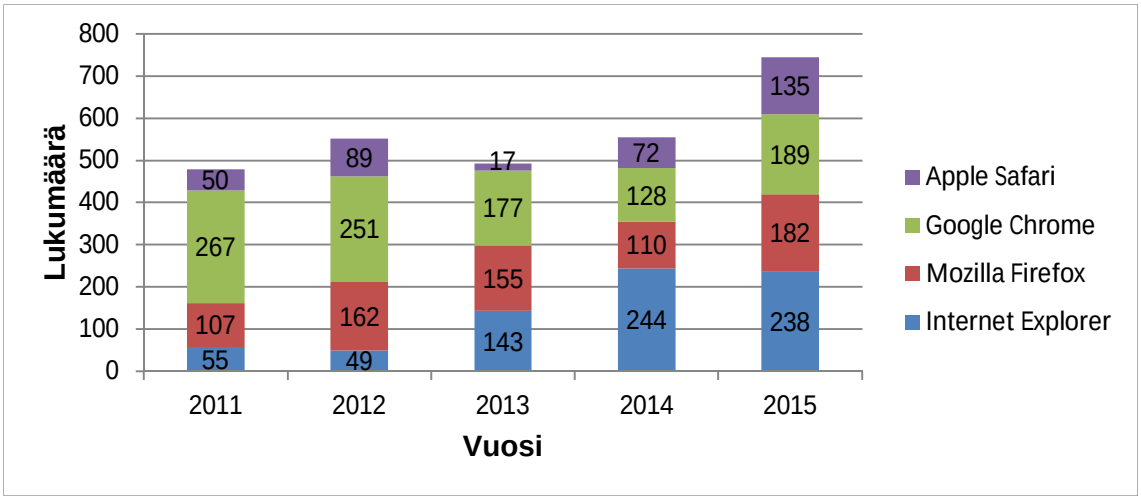
Kuvio 1. Vuosittain julkaistut haavoittuvuudet vakavuusluokittain (NVD 2016)

Kuvioon 2 on haettu Kansallisesta haavoittuvuustietokannasta kaikkien käytetyimpien käyttöjärjestelmien julkaistut haavoittuvuudet vuosilta 2011–2015. Kuviossa 2 on nähtävissä, että vuonna 2015 ollut erittäin paljon haavoittuvuuksien löydöksiä, tämä johtuu siitä, että vuodesta 2015 alkaen Flash Player -liitännäinen on luokiteltu osaksi käyttöjärjestelmää.



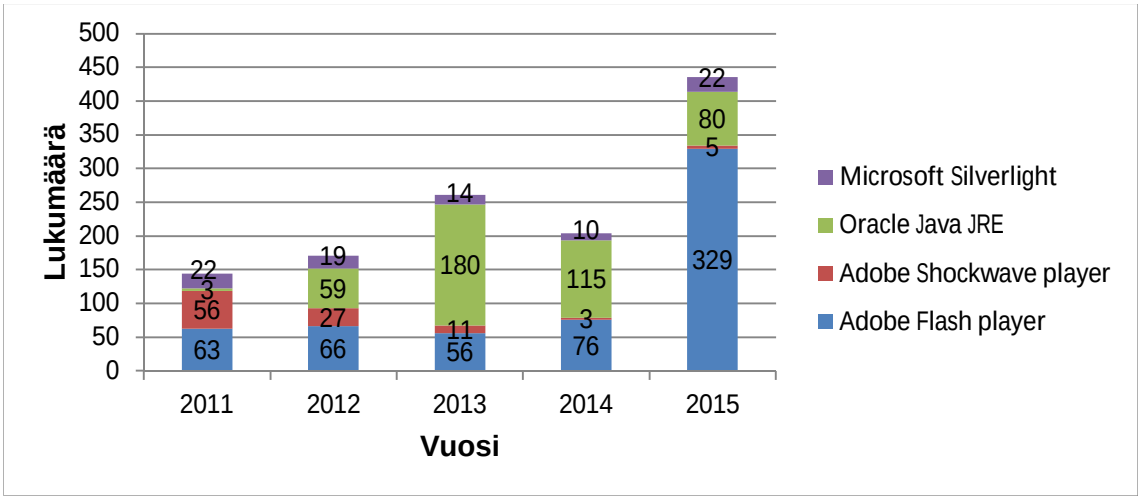
Kuvio 2. Vuosittain julkaistut haavoittuvuudet käyttöjärjestelmittäin (NVD 2016)

Kuvioon 3 on haettu Kansallisesta haavoittuvuustietokannasta käytetyimpien nettiselainten julkaistut haavoittuvuudet vuosilta 2011–2015. Kuviossa 3 on nähtävissä, että haavoittuvuuksien löydökset kasvaneet tasaisesti vuosittain melkein kaikissa selaimissa.



Kuvio 3. Vuosittain julkaistut haavoittuvuudet selaimittain (NVD 2016)

Kuvioon 4 on haettu Kansallisesta haavoittuvuustietokannasta käytetyimpien selainliitännäisten julkaistut haavoittuvuudet vuosilta 2011–2015. Kuviossa 4 esitetään, että vuonna 2015 ollut dramaattinen kasvu Adobe Flash Player haavoittuvuuksien löydöksissä.



Kuvio 4. Vuosittain julkaistut haavoittuvuudet liitännäisittäin (NVD 2016)

3 System Center Configuration Manager 2012

Microsoftin System Center -hallintaratkaisuiden tuoteperheeseen kuuluva Configuration Manager 2012 -järjestelmä, tarjoaa kasvua IT-tuottavuuteen ja tehokkuuteen vähentämällä manuaalisia tehtäviä, maksimoimalla sovellus- ja laitteistoinvestoinnit sekä kasvattamalla käyttäjien tuottavuutta, tarjoamalla tarkoituksen mukaiset sovellukset oikealla hetkellä. SCCM 2012 helpottaa tuottamaan tehokkaampia IT-palveluita turvallisella ja skaalautuvalla sovellusjakelulla, vaatimuksenmukaisuuden asetustenhallinnalla sekä kattavalla palvelinten, työasemien, kannattavien ja mobiililaitteiden laitetietojenhallinnalla. (Microsoft 2015.)

3.1 System Center Configuration Manager 2012 hyödyt

Microsoftin (2016, 2) mukaan SCCM 2012 tuo muun muassa seuraavia hyötyjä, käyttäjät voivat itse asentaa tarvitsemansa ohjelmat yrityksen portaalista kaikille alustoille. Yhtenäinen hallinta niin työasemille, palvelimille, Macintoshille ja Linuxille sekä myös mobiililaitteille, SCCM 2012 ei ilman lisäosia tue mobiililaitteita kuin perustasolla. Vähentää fyysisten palvelinten sekä ensi- ja toissijaisten saittien määrää, tukee myös saittien asentamisen Azure-virtuaalikoneiksi. Parantaa ympäristön toimivuutta asettamalla ja pakottamalla konfiguraatioita, laukaisemalla hälytyksiä virheistä ja tuomalla paremman raportoinnin. Auttaa ylläpitoa toimittamaan sovellukset käyttäjille parhaan toimitustavan mukaisesti eri alustoille. Tuki käyttöjärjestelmien erilaisille asennustekniikoille mm. PXE -käynnistys, verkkoperustainen monilähetys, paikallinen asennus ja käyttöjärjestelmän päivitys. Tunnistaa laitteet joista puuttuu tietoturvapäivityksiä, toimittaa ja asentaa tarvittavat tietoturvapäivitykset ja luo asennuksista raportin. Näyttää konsolissa asiakaskoneiden kunnon, päivitysstatuksen, määritetyt hälytykset sekä laitteisto- ja sovellusluettelon.

3.2 System Center Updates Publisher 2011

SCUP 2011 on erillistyökalu jonka avulla yksityiset sovellustoimittajat tai sovelluksien kehittäjät voivat tuoda sovelluspäivityksiä ulkopuolisista sovelluskatalogeista, luoda tai muokata sovelluspäivitysten määrityksiä, viedä sovelluspäivityksiä ulkopuolisiin sovelluskatalogeihin ja julkaista sovelluspäivityksiä päivityspalvelimelle. Käyttämällä SCUP 2011:sta sovelluspäivitysten hallintaan ja julkaisuun päivityspalvelimelle, ylläpitäjät voivat havaita ja jaella sovelluspäivityksiä työasemille ja palvelimille SCCM 2012:lla. SCUP 2011 tukee sovelluspäivityksiä, joilla on riippuvuuksia kuten laitteisto-ohjaimia ja monen päivityksen päivityspaketteja. (Microsoft 2011b.)

Microsoftin (2011b) mukaan ylläpitäjät voivat tehdä SCUP 2011:lla muun muassa seuraavia asioita, tuoda sovelluskatalogeja, jotka ovat kolmannen osapuolen organisaatioiden luomia tai jotka on luotu ylläpitäjän organisaatiossa. Luoda sovelluspäivitysten soveltuvuuteen ja jakeluun liittyvää kuvaustietoa. Viedä sovelluskatalogeja, että niitä voidaan käyttää toisessa ympäristössä, sekä hallita sovelluspäivitysten tietoja.

4 Sovelluspäivitysten levityksen hallinta

Projektin toimeksiantajana toimii suomalainen sairaanhoitopiiri, jossa työskentelee yli 22000 henkilöä. Sen tietohallinnossa on yli 200 asiantuntijaa. Sairaanhoitopiirin palveluita käytti vuonna 2015 noin 485000 eri henkilöä. Sen työasemaympäristössä on noin 19000 työasemaa ja niihin kuuluu niin kannettavia kuin pöytätietokoneita.

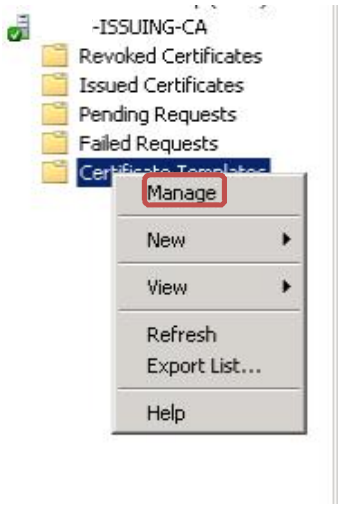
4.1 Projektisuunnitelma

Projektin tavoitteena on tehdä käyttöönottosuunnitelma SCUP 2011:lle tuotantoympäristöön. Testiympäristön asennuksiin, määrityksiin ja itse tuotoksen testauksiin menee yhteensä noin kaksi kuukautta (työtä tehdään maksimissaan 8 tuntia viikossa) eli yhteensä noin 8 henkilötyöpäivää. Testiympäristössä on AD (Active Directory) -palvelu, GPO:t (Group Policy Object) vastaavat tuotannon GPO:a. SCUP 2011:n asennus vaatii jonkin verran AD -operointia, esimerkiksi muutaman GPO:n tekemistä ja julkaisua. Allekirjoitusvarmenne luodaan CA:lla (Certificate Authority), mikä on AD CS (Active Directory Certificate Services) -palvelu. Testiympäristöstä on estetty pääsy tuotantoympäristön palveluihin, joten virheellisillä määrityksillä ei voida sotkea tuotantoympäristön toiminnallisuutta. Testiympäristöön asennetaan myös kaksi virtuaalista työasemaa, joihin testijakelut tehdään, yhdellä työasemalla myös haetaan CA:lla julkaistu varmenne ja tallennetaan se paikallisesti työasemalle jatkokäsittelyä varten. Tuotoksena testauksista saadaan SCUP 2011 käyttöönottosuunnitelma kuvankaappauksineen, minkä perusteella kuka vaan kellä on oikeudet, voi asennuksen tehdä.

4.2 Toteutus

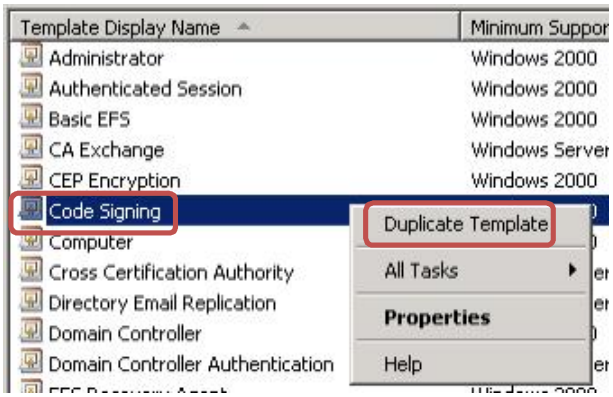
Ensimmäisenä asennettiin kaksi Windows 7 -virtuaalityöasemaa, sekä 32- että 64-bittinen. Asennukset tehtiin perusasetuksilla, asennuksen jälkeen ne liitettiin testiympäristön toimialueeseen. Tämän jälkeen luotiin allekirjoitusvarmenne, millä SCUP 2011 allekirjoittaa julkaisemansa paketit, tällä tavoin saatiin työasemat luottamaan paketin julkaisijan ympäristöön. Varmenne luotiin CA:lla ja se määritettiin haettavaksi toimialueen käyttäjille.

Aukaistiin CA ja painettiin oikealla hiirennapilla ”Certificate Templates” -kansiota, aukeavasta listasta valittiin ”Manage”, kuten kuviossa 5 on esitetty.



Kuvio 5. Varmennepohjien hallintaikkunan aukaisu

Aukeavasta ikkunasta painettiin oikealla hiirennapilla ”Code Signing” -varmennepohjaa ja aukeavasta listasta valittiin ”Duplicate Template”, kuten kuviossa 6 on esitetty.

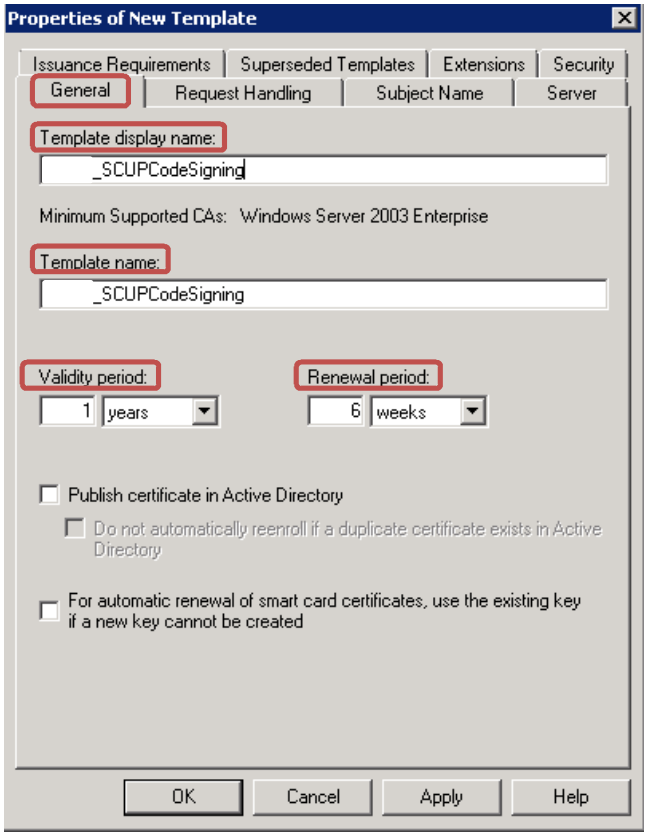


Kuvio 6. ”Code Signing” -varmennepohjan kaksoiskappaleen teko

Aukeavasta ikkunasta valittiin ”Windows Server 2003 Enterprise” ja painettiin ”OK”-painiketta, kuten kuviossa 7 on esitetty.

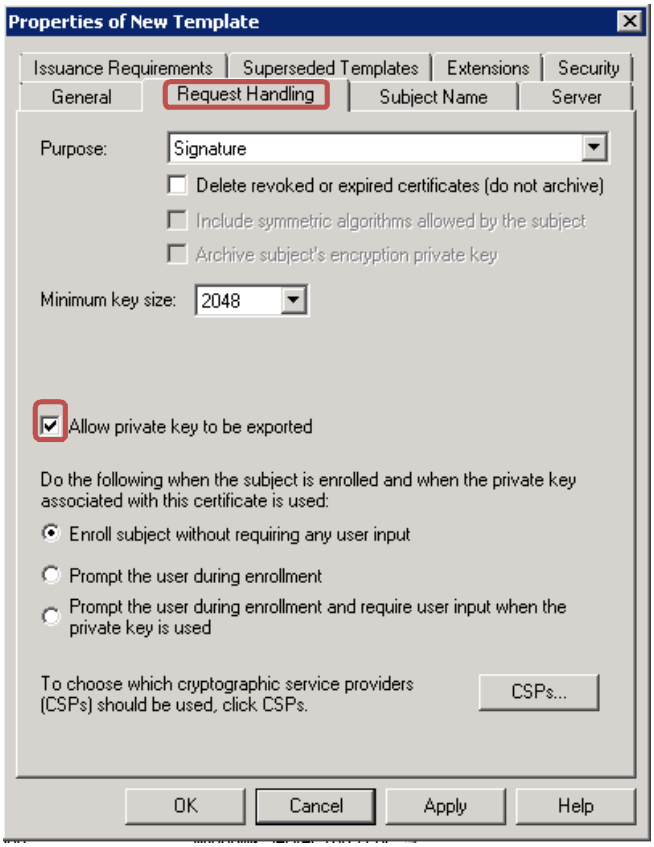
Kuvio 7. CA:n versiotuen valinta

Aukeavasta ikkunasta valittiin ”General”-välilehti ja kirjoitettiin nimi varmennepohjalle kohtiin ”Template display name” ja ”Template name”, määritettiin sertifikaatille olemassaolo- ja uusinta-aika kohtiin ”Validity period” ja ”Renewal period”, kuten kuviossa 8 on esitetty.



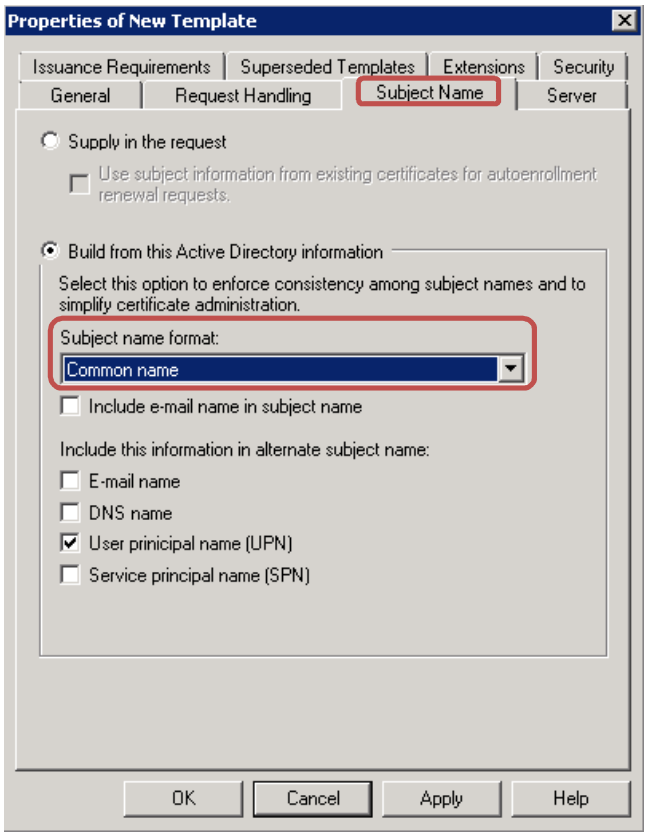
Kuvio 8. Varmennepohjan yleiset määritykset

Seuraavaksi valittiin ”Request Handling” -välilehti ja laitettiin ruksi kohtaan “Allow private key to be exported”, kuten kuviossa 9 on esitetty.



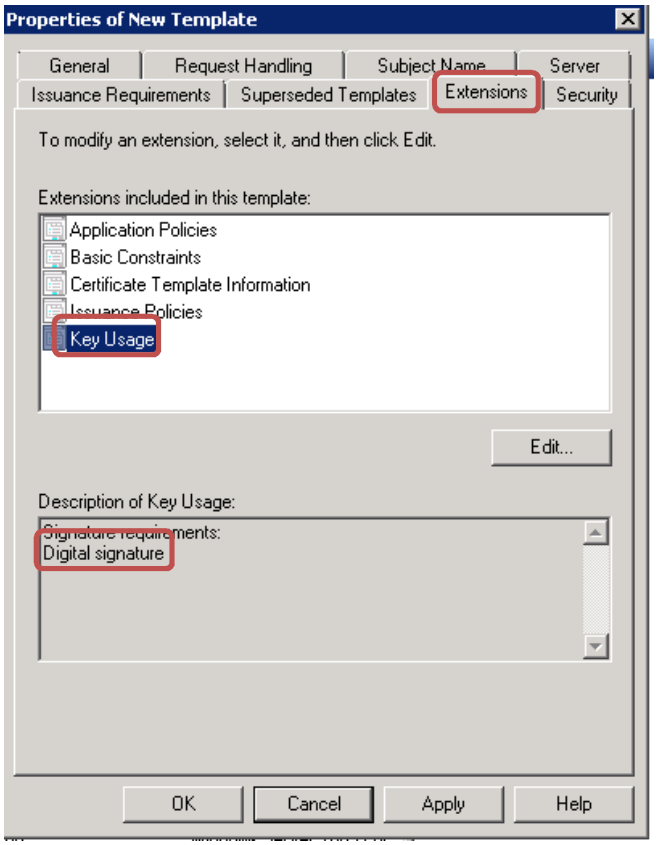
Kuvio 9. Sallitaan yksityisen avaimen tallentaminen

Seuraavaksi valittiin ”Subject Name” -välilehti ja ”Subject name format” -pudotusvalikosta muutettiin arvoksi ”Common name”, kuten kuviossa 10 on esitetty.



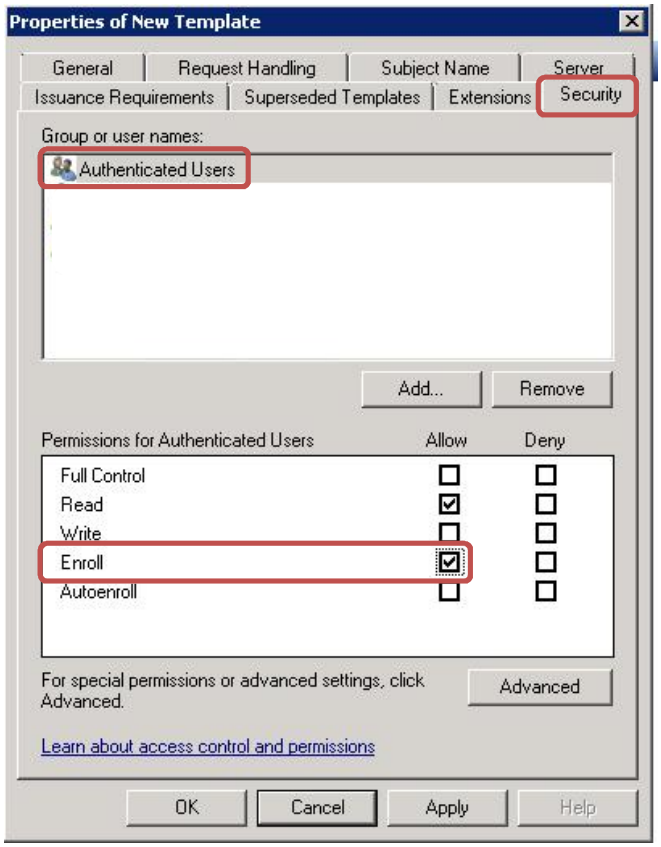
Kuvio 10. “Subject name format” -arvon määritys

Seuraavaksi valittiin ”Extensions”-välilehti ja tarkistettiin että ”Key Usage” on ”Digital signature”, kuten kuviossa 11 on esitetty.



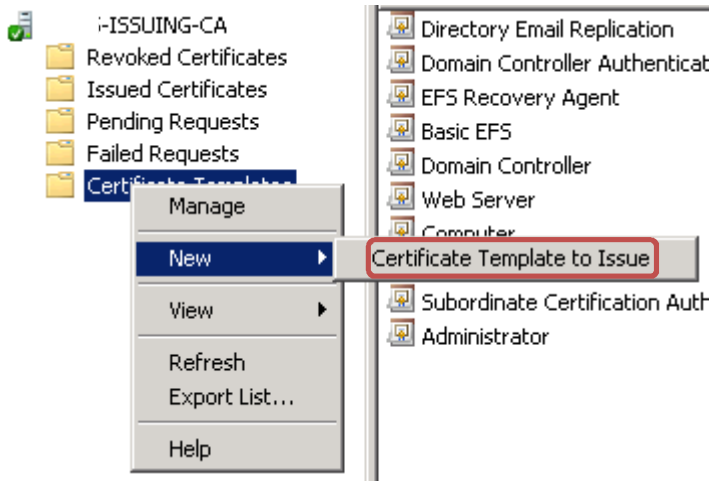
Kuvio 11. ”Key Usage” -arvon tarkistaminen

Seuraavaksi valittiin ”Security”-välilehti ja tarkistettiin että ”Authenticated Users” -käyttäjäryhmällä on ”Enroll”-oikeudet, kuten kuviossa 12 on esitetty.



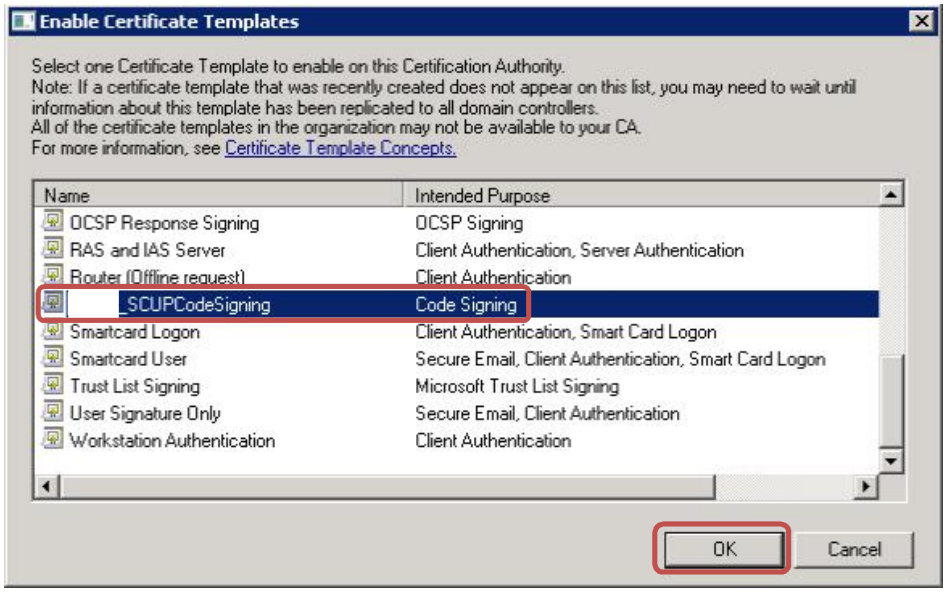
Kuvio 12. Käyttäjäoikeuksien tarkistaminen

Lopuksi painettiin ”OK”-painiketta ja suljettiin varmennepohjien hallintakonsoli. Seuraavaksi juuri luotu varmennepohja julkaistiin. Julkaisu tehtiin painamalla oikealla hiirennapilla CA:n ”Certificate Templates” -kansiota ja aukeavasta listasta valittiin ”New” ja sieltä ”Certificate Template to Issue”, kuten kuviossa 13 on esitetty.



Kuvio 13. Varmennepohjan julkaisun aloitus

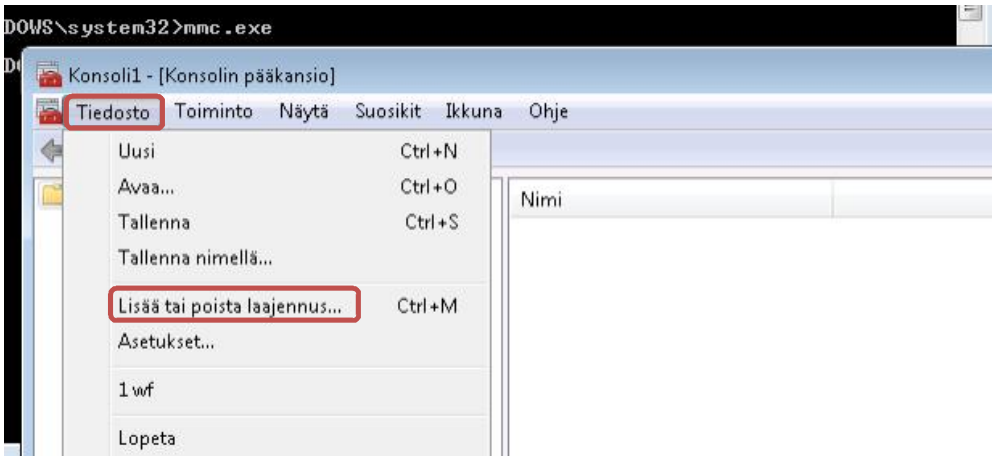
Aukeavasta ikkunasta valittiin juuri luotu varmennepohja ja painettiin ”OK”-painiketta, kuten kuviossa 14 on esitetty.



Kuvio 14. Julkaistavan varmennepohjan valinta

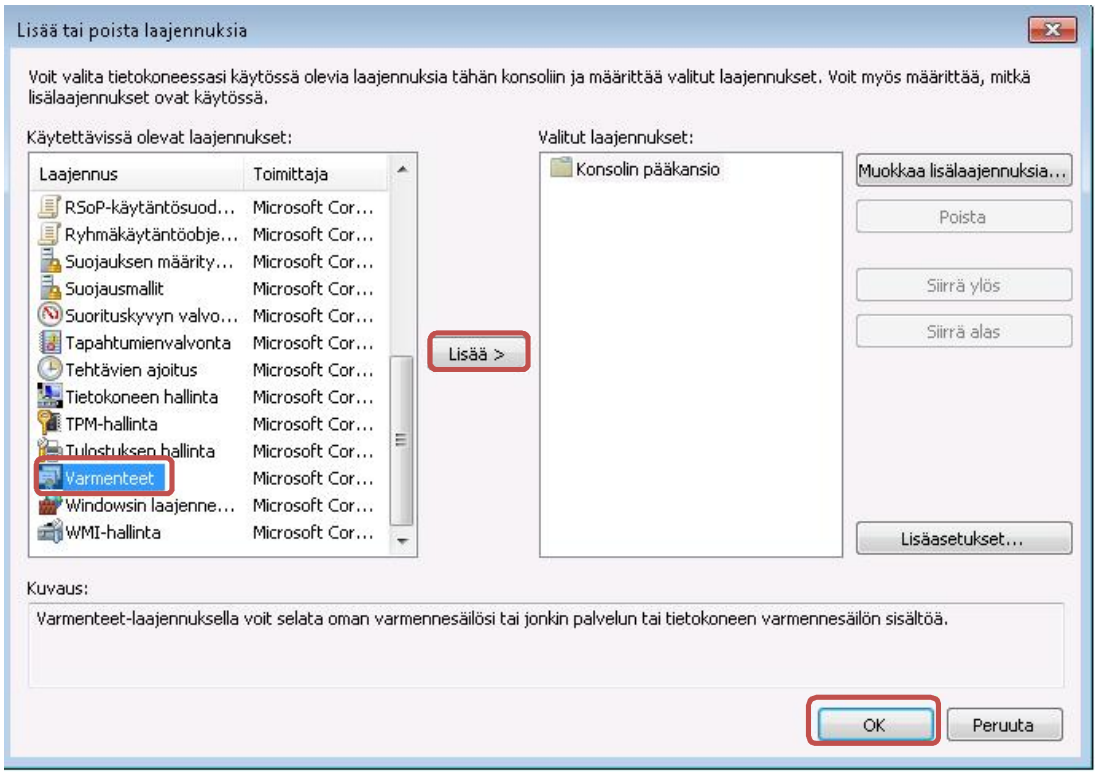
Seuraavaksi haettiin julkaistu varmennepohja toimialueella olevaan työasemaan ja tallennettiin varmenne sekä varmenteen yksityinen avain työasemalle.

Aukaistiin MMC (Microsoft Management Console) järjestelmänvalvojan oikeuksilla ja valittiin aukeavasta ikkunasta ”Tiedosto” ja aukeavasta listalta ”Lisää tai poista laajennus…”, kuten kuviossa 15 on esitetty.



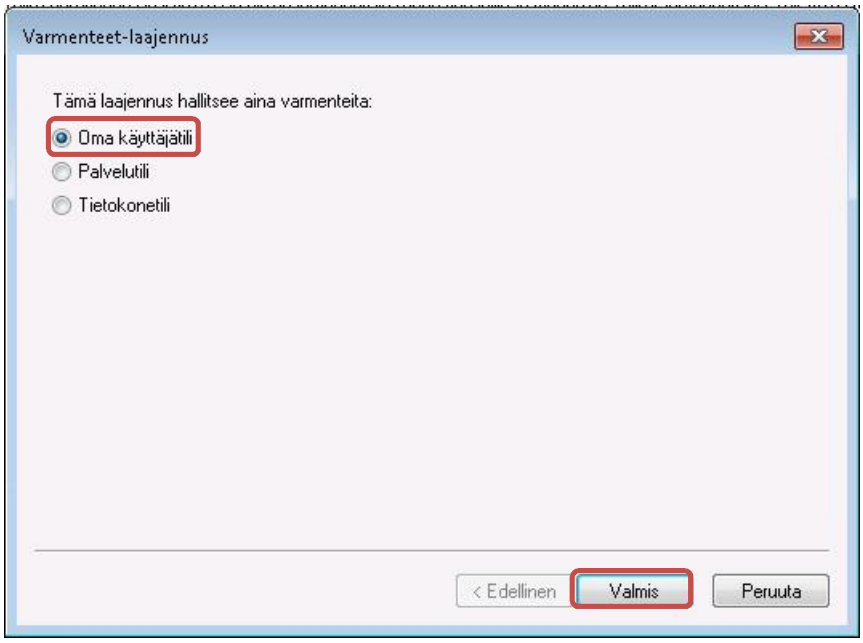
Kuvio 15. Laajennuksen lisäys hallintakonsoliin

Aukeavan ikkunan vasemman puolimmaisesta listasta valittiin ”Varmenteet” ja painettiin ”Lisää >” -painiketta, kuten kuviossa 16 on esitetty.



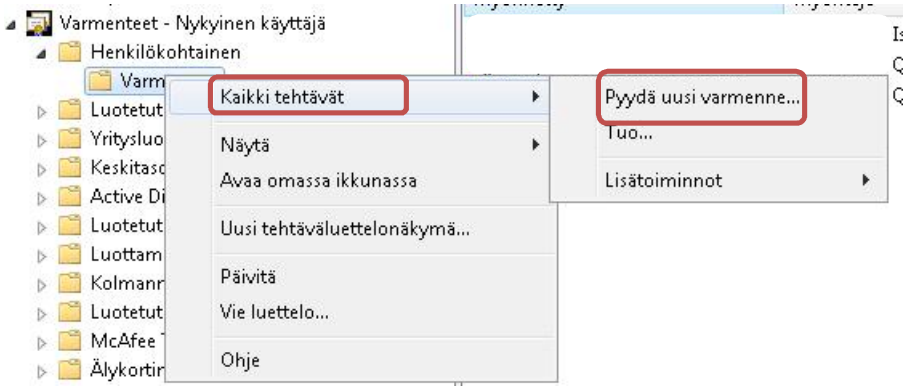
Kuvio 16. Varmenteet laajennuksen lisäys

Aukeavasta ikkunasta valittiin ”Oma käyttäjätili” ja painettiin ”Valmis”-painiketta, kuten kuviossa 17 on esitetty. Sulje ”Lisää tai poista laajennuksia” -ikkuna painamalla ”OK”-painiketta (kuvio 16).



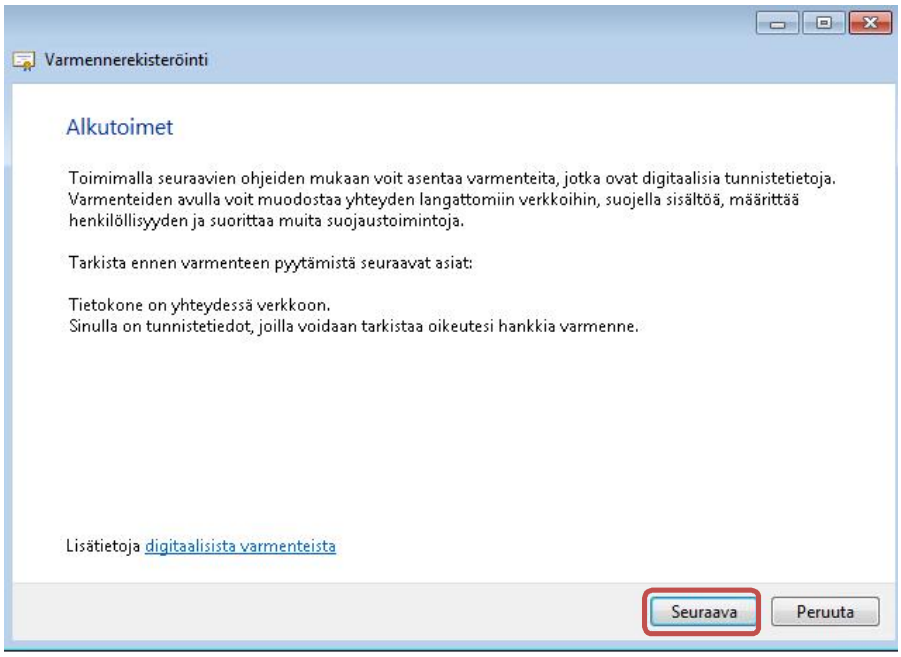
Kuvio 17. Laajennuksen määritys

Aukeavasta ikkunasta tekstin vasemmalla olevasta nuolesta ensin laajennettiin ”Varmenteet – Nykyinen käyttäjä” -kansio ja sitten ”Henkilökohtainen”-kansio. ”Henkilökohtainen”-kansion alta painettiin oikealla hiiren napilla ”Varmenteet”-kansiota, aukeavasta listasta valittiin ”Kaikki tehtävät” ja sieltä ”Pyydä uusi varmenne…”, kuten kuviossa 18 on esitetty.



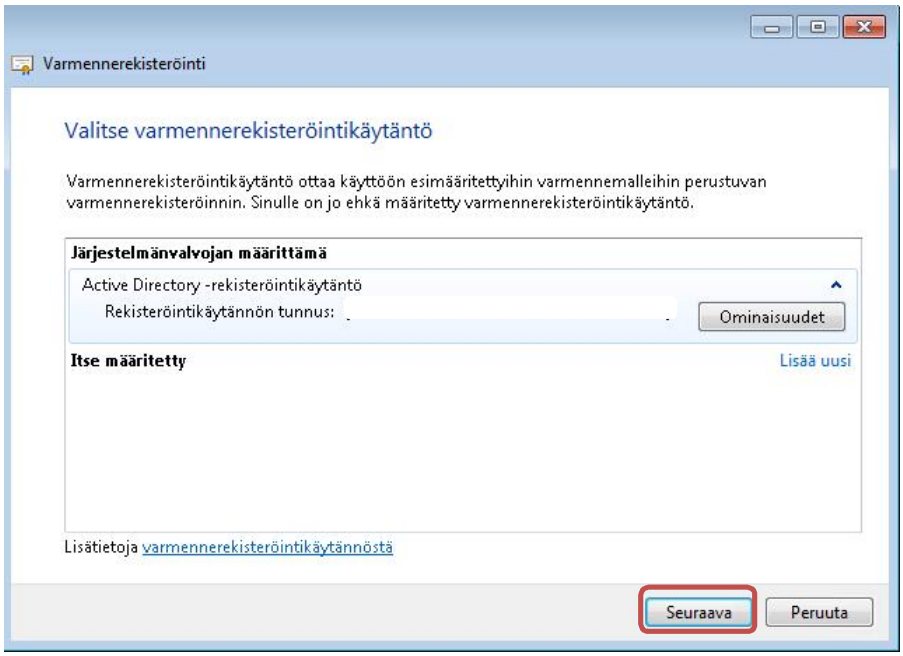
Kuvio 18. Varmenteen haun aloitus

Aukeavasta ikkunasta painettiin ”Seuraava”-painiketta, kuten kuviossa 19 on esitetty.



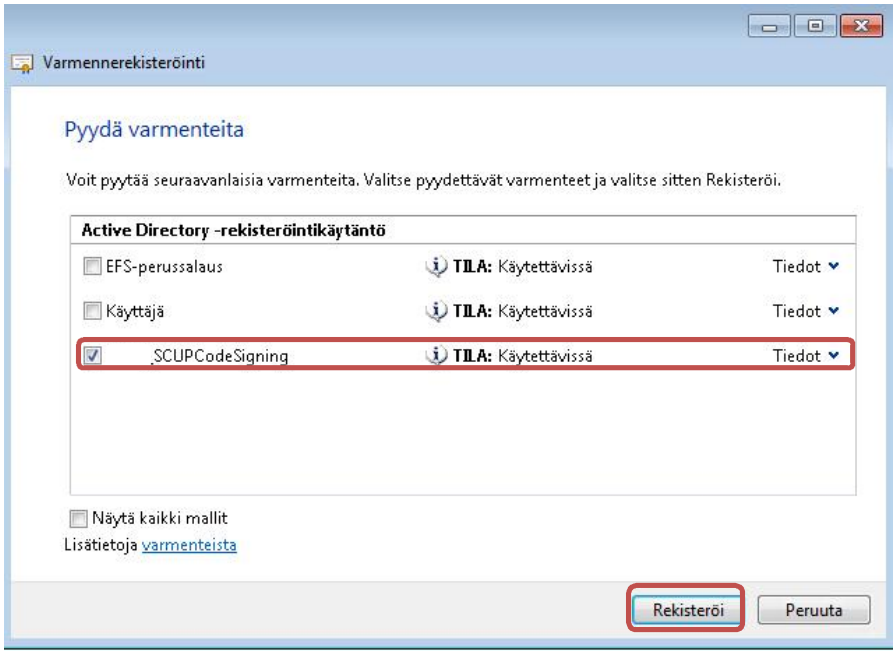
Kuvio 19. Varmenteen rekisteröinnin aloitus

Seuraavassa ikkunassa painettiin ”Seuraava”-painiketta, kuten kuviossa 20 on esitetty.



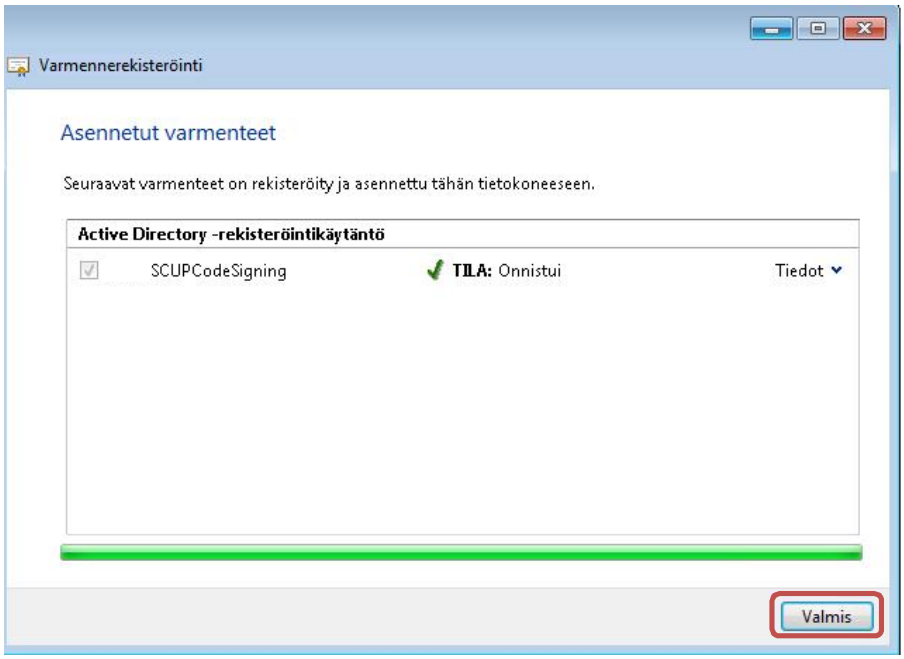
Kuvio 20. Rekisteröintikäytännön valinta

Seuraavassa ikkunassa valittiin varmenne, mikä aikaisemmin luotiin ja painettiin ”Rekisteröi”-painiketta, kuten kuviossa 21 on esitetty.



Kuvio 21. Varmenteen valinta

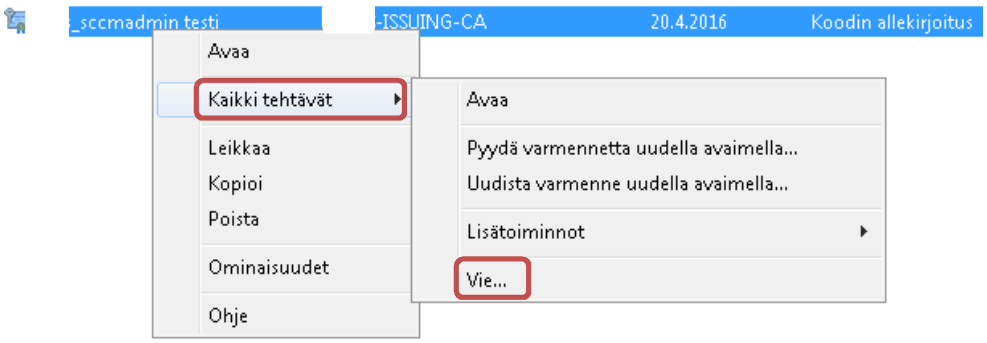
Seuraavassa ikkunassa painettiin ”Valmis”-painiketta, kuten kuviossa 22 on esitetty.



Kuvio 22. Varmenteen asennus valmis

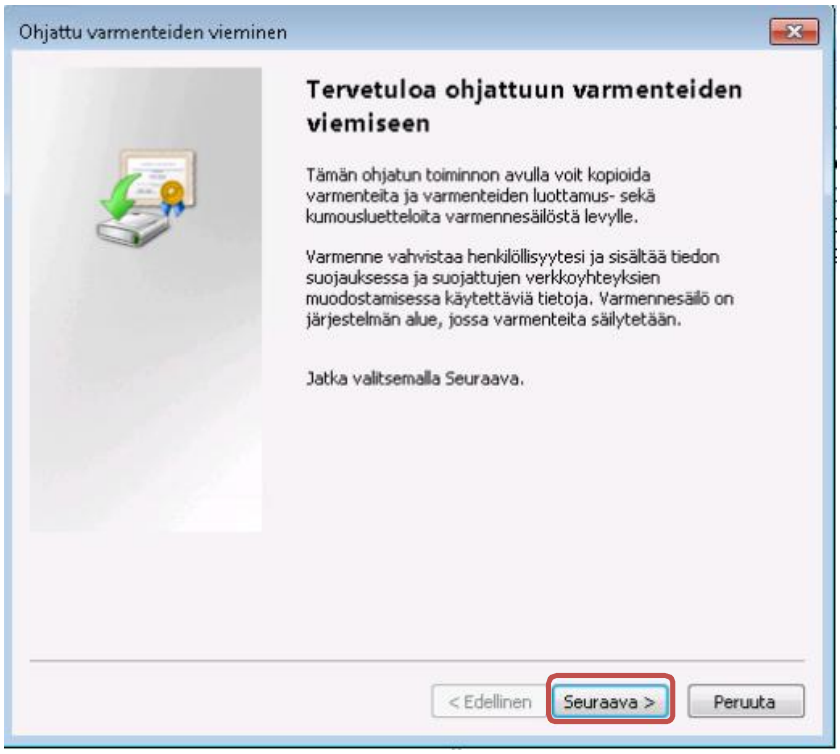
Seuraavaksi varmenne tallennettiin työasemalle. Varmenne löytyy ”Henkilökohtainen”-kansion alla olevasta ”Varmenteet”-kansiosta ja se on nimetty käyttäjänimen mukaan. Jos varmenteen nimeä halutaan muuttaa pitää se tehdä edellisten toimenpiteiden aikana ”Tiedot”-valikossa, joka löytyy varmenteen tilan jälkeen kuviosta 21.

Painettiin oikealla hiirennapilla varmennetta ja valittiin listasta ”Kaikki tehtävät” ja sieltä ”Vie…”, kuten kuviossa 23 on esitetty.



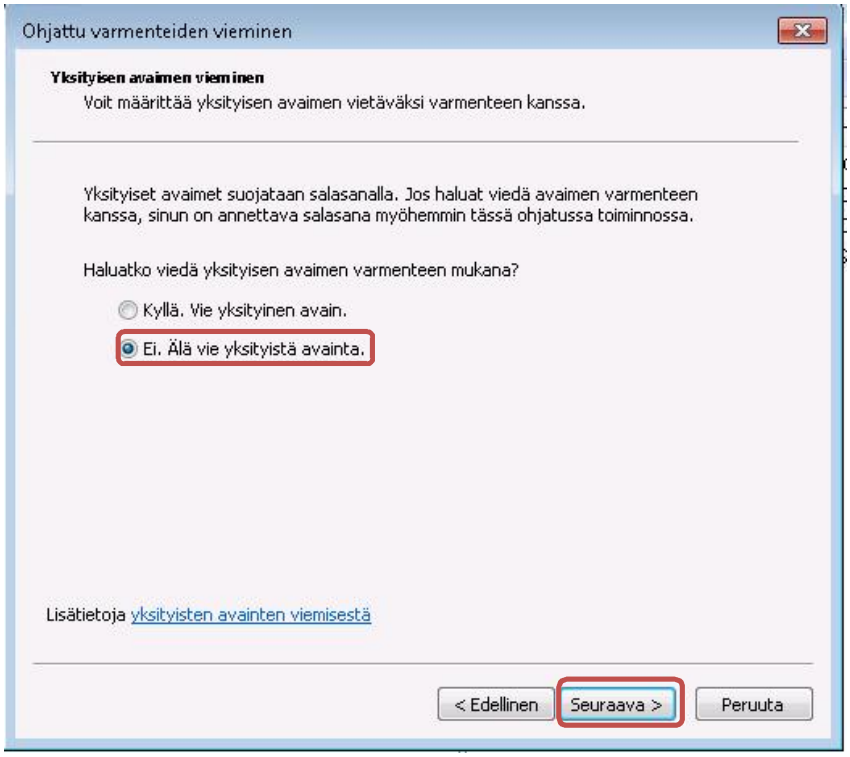
Kuvio 23. Varmenteen tallennuksen aloitus

Aukeavasta ikkunasta painettiin ”Seuraava >”-painiketta, kuten kuviossa 24 on esitetty.



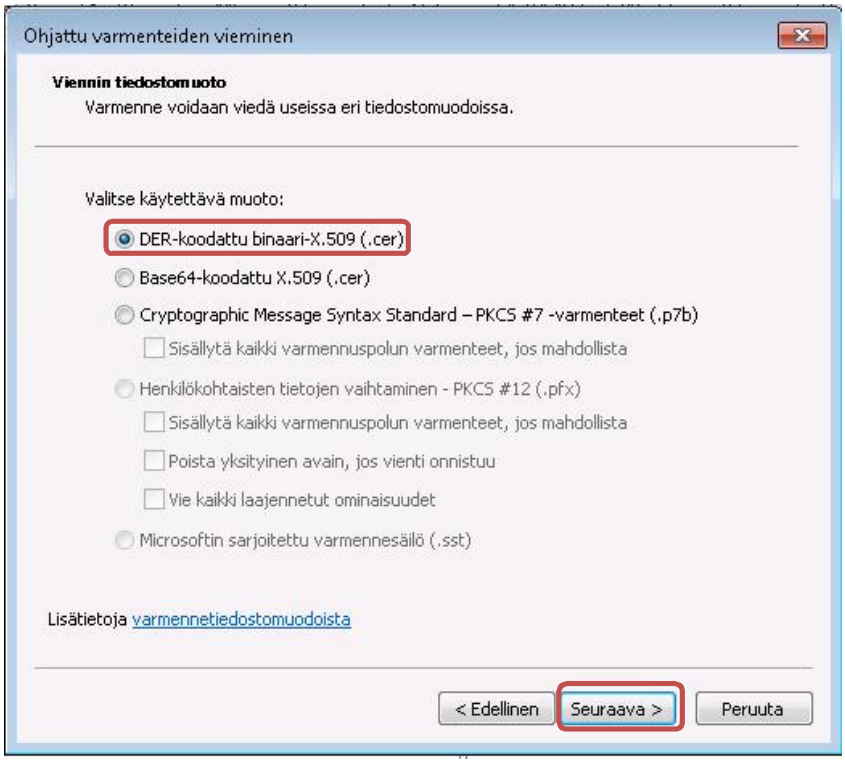
Kuvio 24. Ohjattu varmenteiden vieminen

Seuraavasta ikkunasta valittiin ”Ei. Älä vie yksityistä avainta.” ja painettiin ”Seuraava >”-painiketta, kuten kuviossa 25 on esitetty.



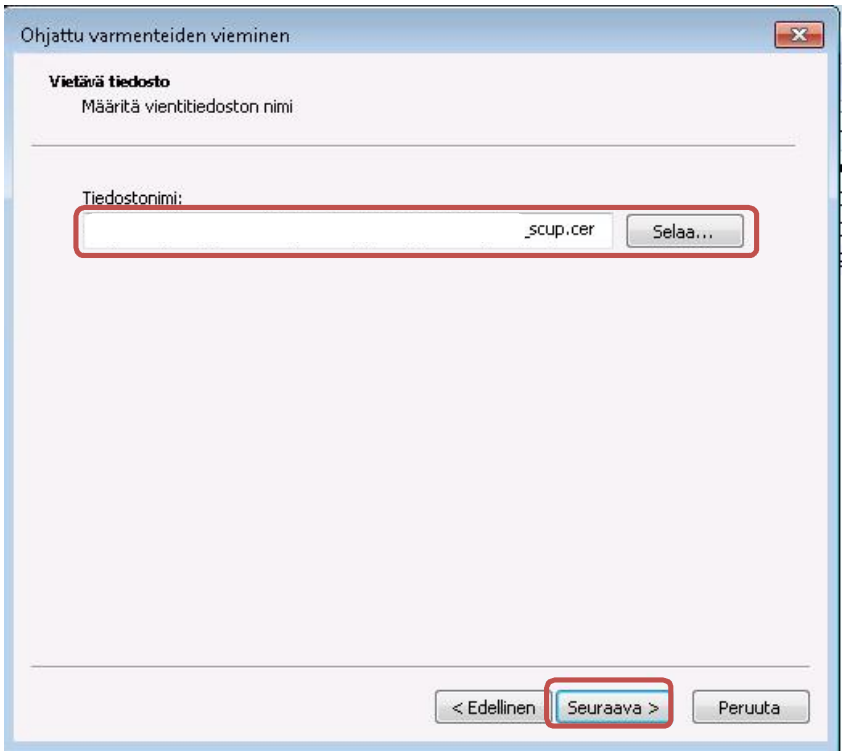
Kuvio 25. Yksityisen avaimen viennin valinta

Seuraavasta ikkunasta valittiin ”DER-koodattu binaari-X.509 (.cer)” ja painettiin ”Seuraava >” -painiketta, kuten kuviossa 26 on esitetty.



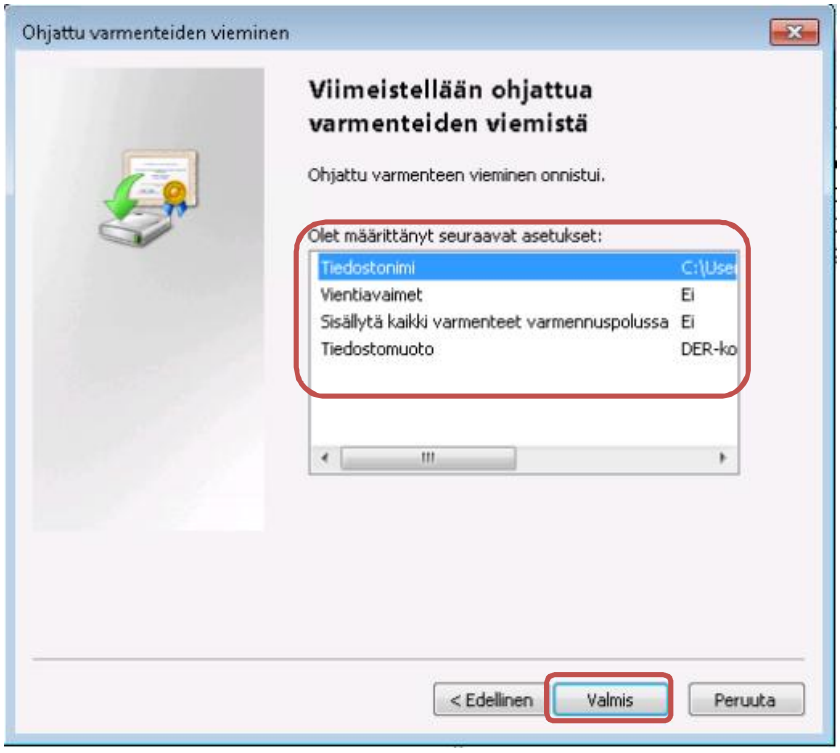
Kuvio 26. Viennin tiedostomuoto

Seuraavassa ikkunassa valittiin tiedostolle nimi, kansio minne tiedosto tallennettiin ja painettiin ”Seuraava >” -painiketta, kuten kuviossa 27 on esitetty.



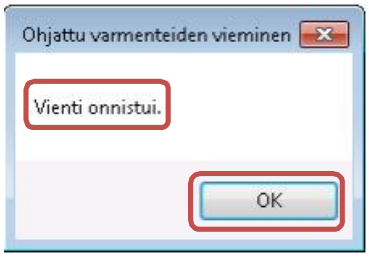
Kuvio 27. Viennin tiedostonimi ja kansio

Seuraavassa ikkunassa tarkistettiin, että tiedot ovat oikein ja painettiin ”Valmis”-painiketta, kuten kuviossa 28 on esitetty.



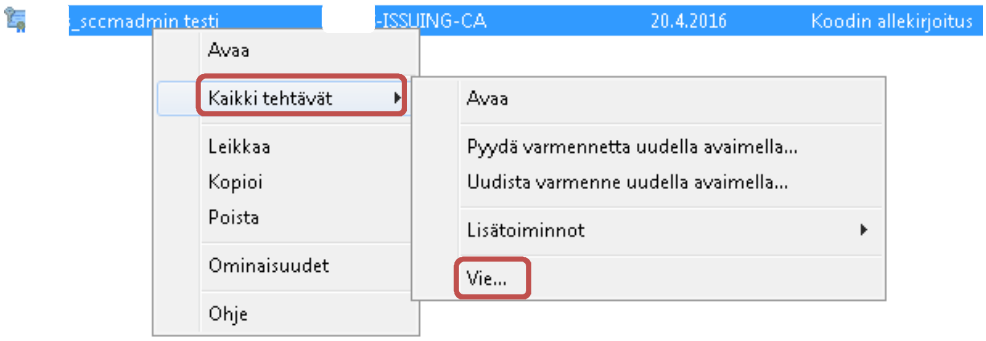
Kuvio 28. Varmenteen viennin viimeistely

Varmenteen viennin pitää onnistua, tästä tuli ilmoitus ja ilmoitusikkunasta painettiin ”OK”-painiketta, kuten kuviossa 29 on esitetty.



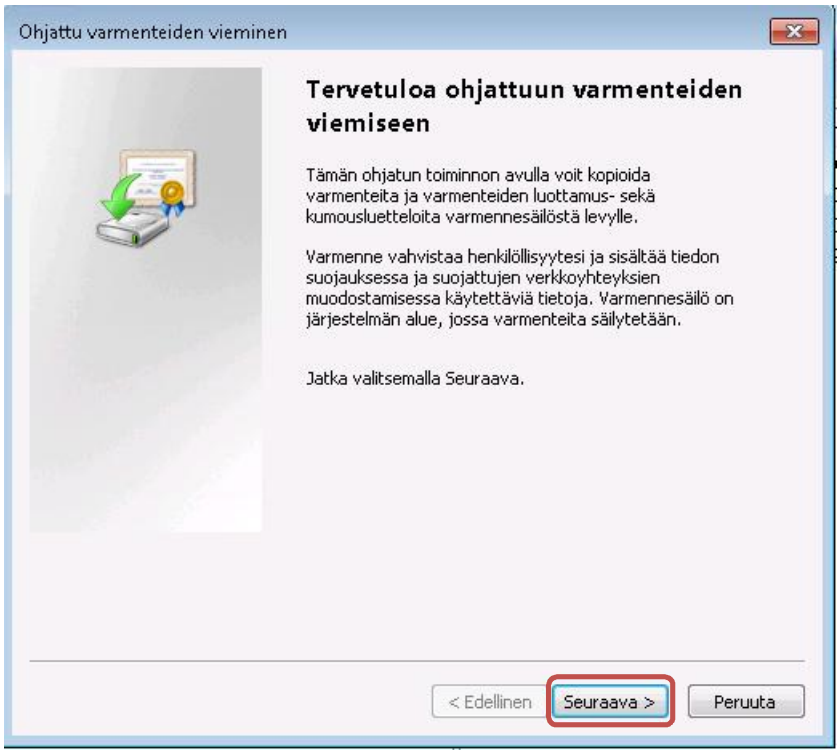
Kuvio 29. Varmenteen viennin onnistuminen

Seuraavaksi vienti aloitettiin alusta ja tällä kertaa vietiin yksityinen avain. Vienti aloitettiin painamalla oikealla hiirennapilla varmennetta ja valittiin aukeavasta listasta ”Kaikki tehtävät” ja sieltä ”Vie…”, kuten kuviossa 30 on esitetty.



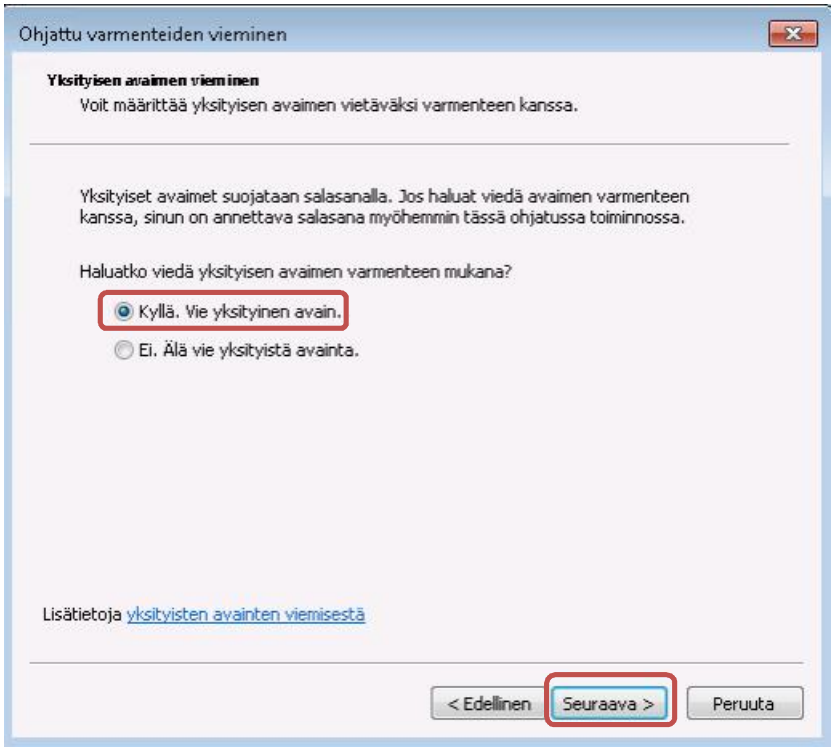
Kuvio 30. Varmenteen viennin aloitus

Seuraavasta ikkunasta painettiin ”Seuraava”-painiketta, kuten kuviossa 31 on esitetty.



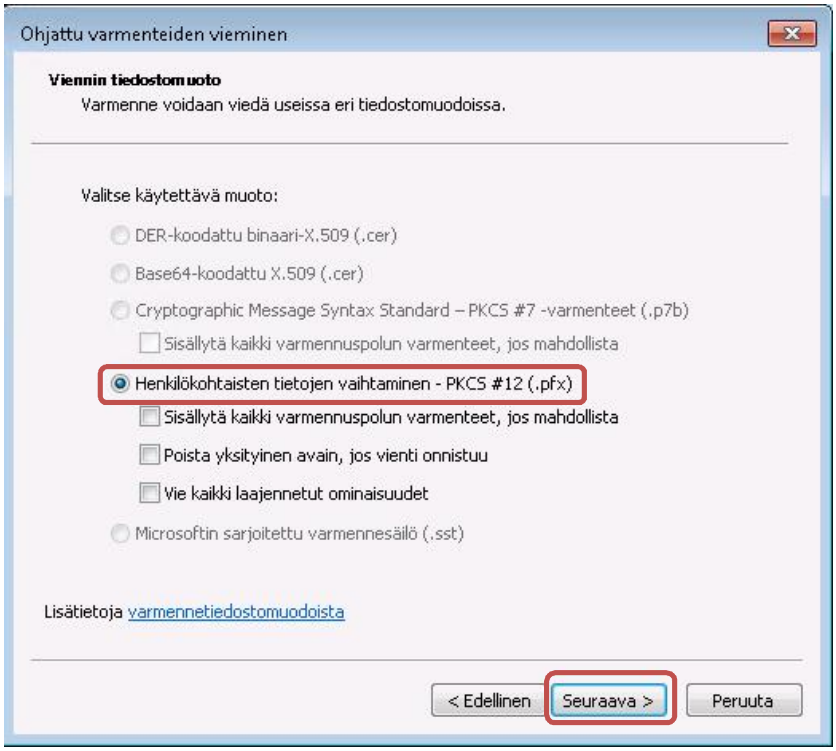
Kuvio 31. Viennin aloitusikkuna

Seuraavassa ikkunassa valittiin ”Kyllä. Vie yksityinen avain” ja painettiin ”Seuraava >” -painiketta, kuten kuviossa 32 on esitetty.



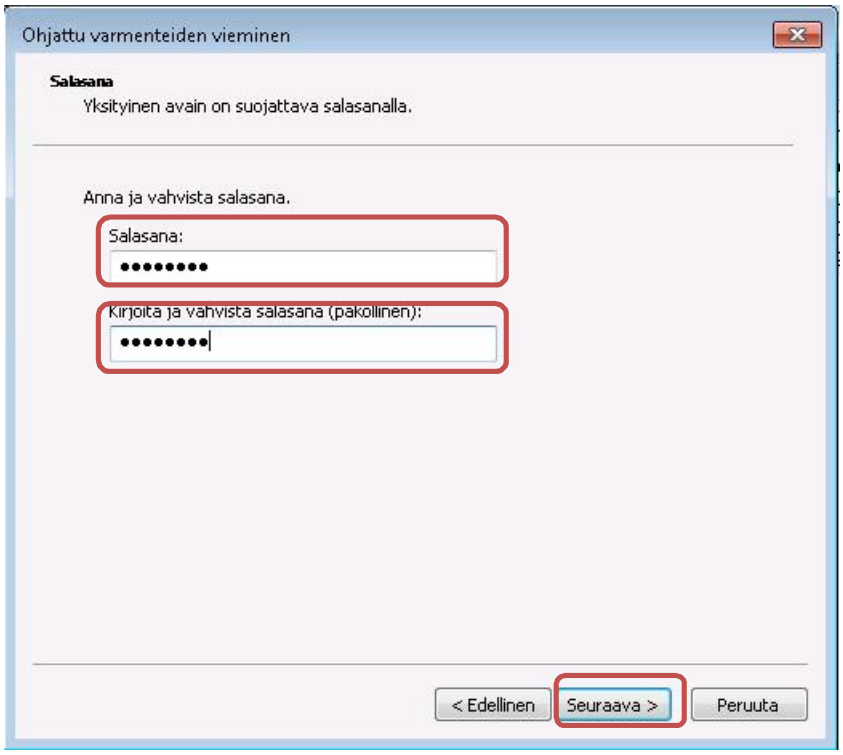
Kuvio 32. Yksityisen avaimen viennin valinta

Seuraavassa ikkunassa valittiin ”Henkilökohtaisten tietojen vaihtaminen – PKCS # 12 (.pfx)” ja painettiin ”Seuraava >” -painiketta, kuten kuviossa 33 on esitetty.



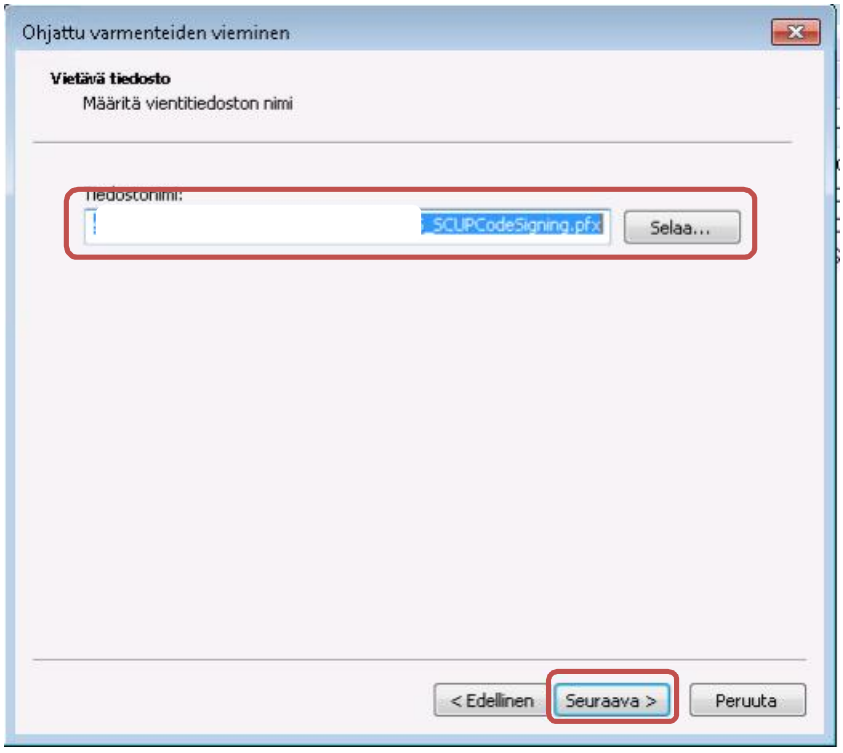
Kuvio 33. Viennin tiedostomuodon valinta

Seuraavassa ikkunassa annettiin yksityiselle avaimelle salasana ja painettiin ”Seuraava >” -painiketta, kuten kuviossa 34 on esitetty.



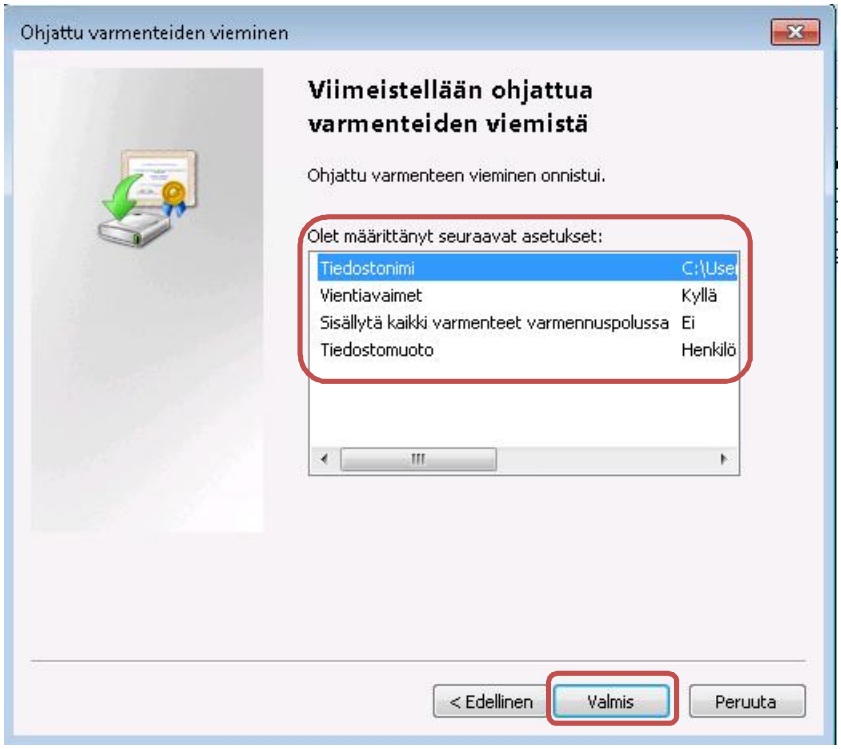
Kuvio 34. Salasanan määritys yksityiselle avaimelle

Seuraavassa ikkunassa tiedostolle annettiin nimi ja kansio, minne tiedosto tallennettiin, lopuksi painettiin ”Seuraava >” -painiketta, kuten kuviossa 35 on esitetty.



Kuvio 35. Yksityisen avaimen tallennus

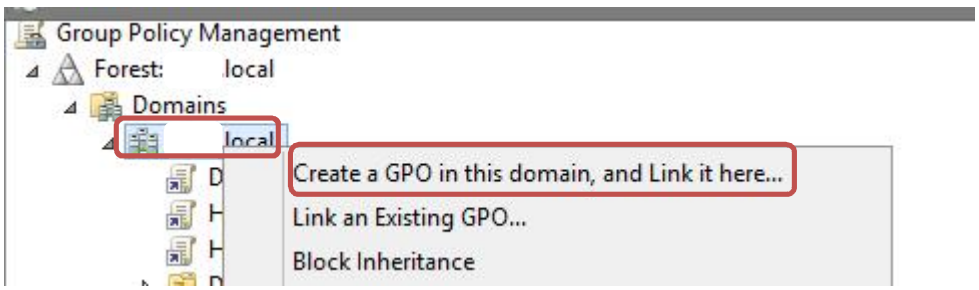
Seuraavassa ikkunassa tarkistettiin, että tiedot ovat oikein ja painettiin ”Valmis”-painiketta, kuten kuviossa 36 on esitetty.



Kuvio 36. Yksityisen avaimen viennin viimeistely

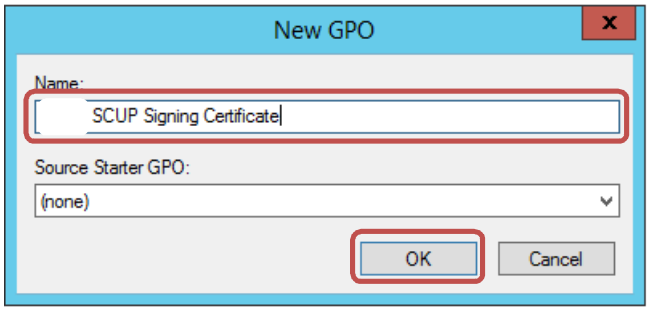
Seuraavaksi tehty varmenne levitettiin kaikille työasemille GPO:lla. Testiympäristössä varmuuden vuoksi varmenne vietiin GPO:lla kansioihin ”Trusted Root (Luotetut varmenteiden päämyöntäjät)” ja ”Trusted Publisher (Luotetut julkaisijat)”, tuotantoympäristöön riittää pelkkä ”Trusted Publisher” -kansioon vienti, jos luottosuhteet ovat oikein määritetty.

Ensimmäisenä avattiin ”Group Policy Management” -työkalu toimialueen ohjauskoneella ja sieltä oikealla hiirennapilla painettiin toimialuetta ja avautuvasta listasta valittiin ”Create a GPO in this domain, and Link it here…”, kuten kuviossa 37 on esitetty.



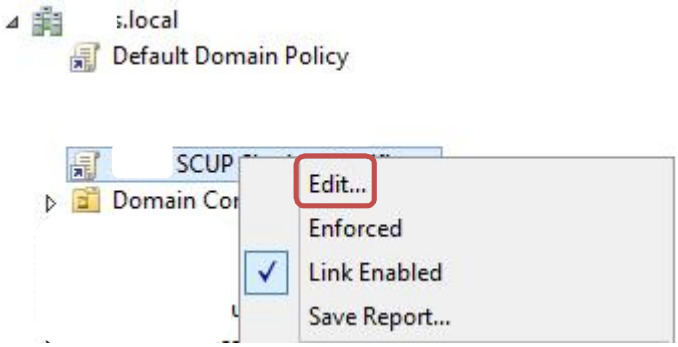
Kuvio 37. Varmennelevityksen GPO:n luonti

Aukeavassa ikkunassa annettiin nimi uudelle GPO:lle ja lopuksi painettiin ”OK”-painiketta, kuten kuviossa 38 on esitetty.



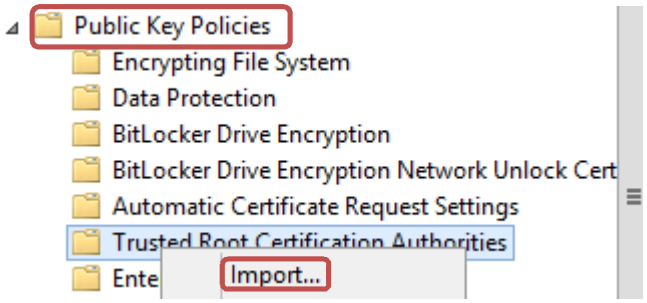
Kuvio 38. GPO:n nimeäminen

Seuraavaksi GPO:a muokattiin. Toimialueen alta painettiin hiiren oikealla napilla juuri tehtyä GPO:a ja aukeavasta listasta valittiin ”Edit…”, kuten kuviossa 39 on esitetty.



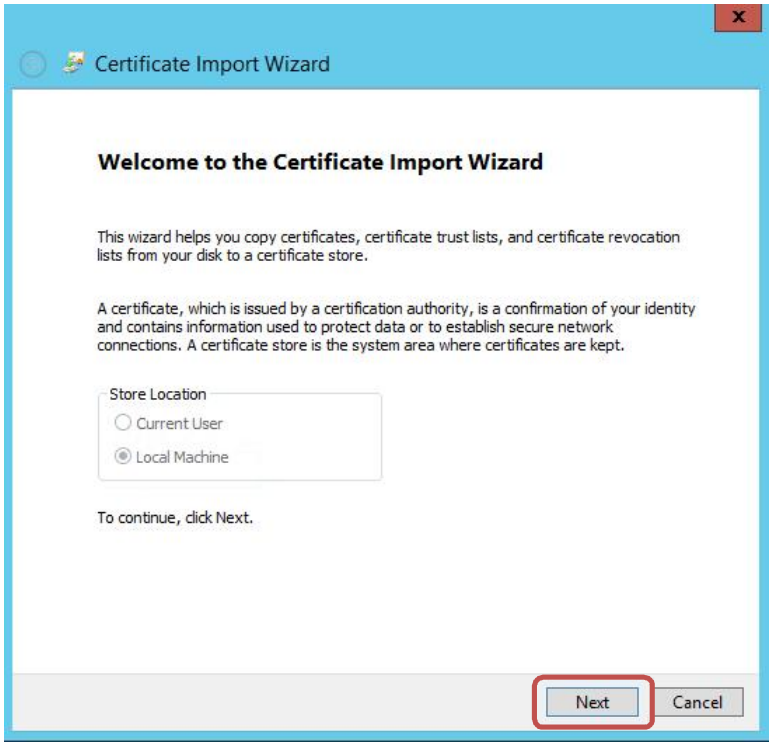
Kuvio 39. GPO:n muokkaamisen aloitus

Aukeavassa ikkunassa navigoitiin ”Windows Settings / Security Settings / Public Key Policies” -kansioon. Siellä varmenne tuotiin ”Trusted Root Certification Authorities” ja ”Trusted Publisher” -kansioihin. Alla olevissa kuvioissa tuonti tehtiin ”Trusted Root Certfication Authorities” -kansioon ja ”Trusted Publisher” -kansioon varmenteen tuonti tapahtuu samalla lailla mutta siitä ei ole kuvia ja se piti kuitenkin tehdä. Kansion päällä painettiin oikeaa hiiren nappia ja aukeavasta listasta valittiin ”Import…”, kuten kuviossa 40 on esitetty.



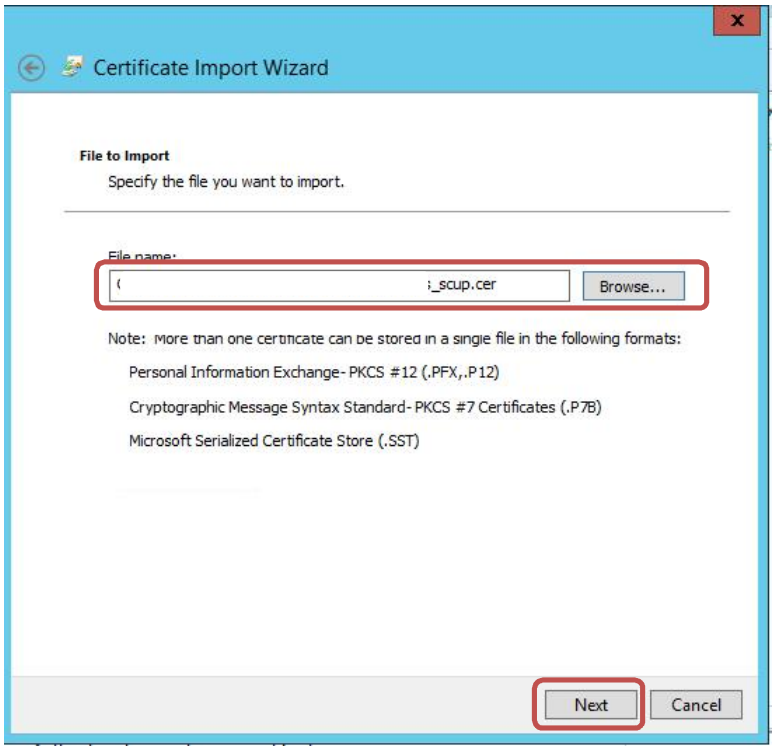
Kuvio 40. Varmenteen tuonnin aloitus

Aukeavasta ikkunasta painettiin ”Next”-painiketta, kuten kuviossa 41 on esitetty.



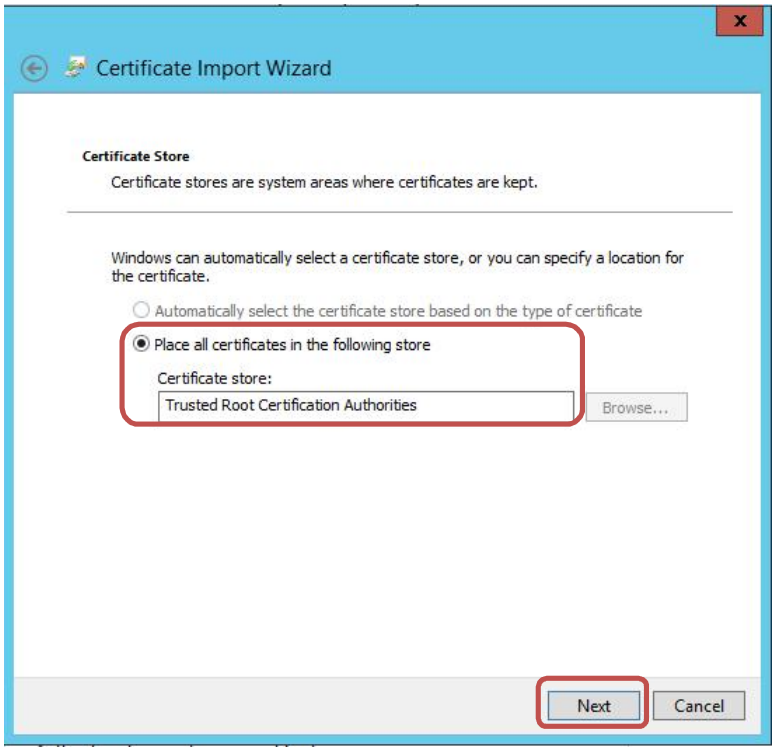
Kuvio 41. Varmenteen tuonti

Seuraavasta ikkunasta haettiin tuotava varmenne ”Browse”-painikkeesta aukeavasta ikkunasta ja haun jälkeen painettiin ”Next”-painiketta, kuten kuviossa 42 on esitetty.



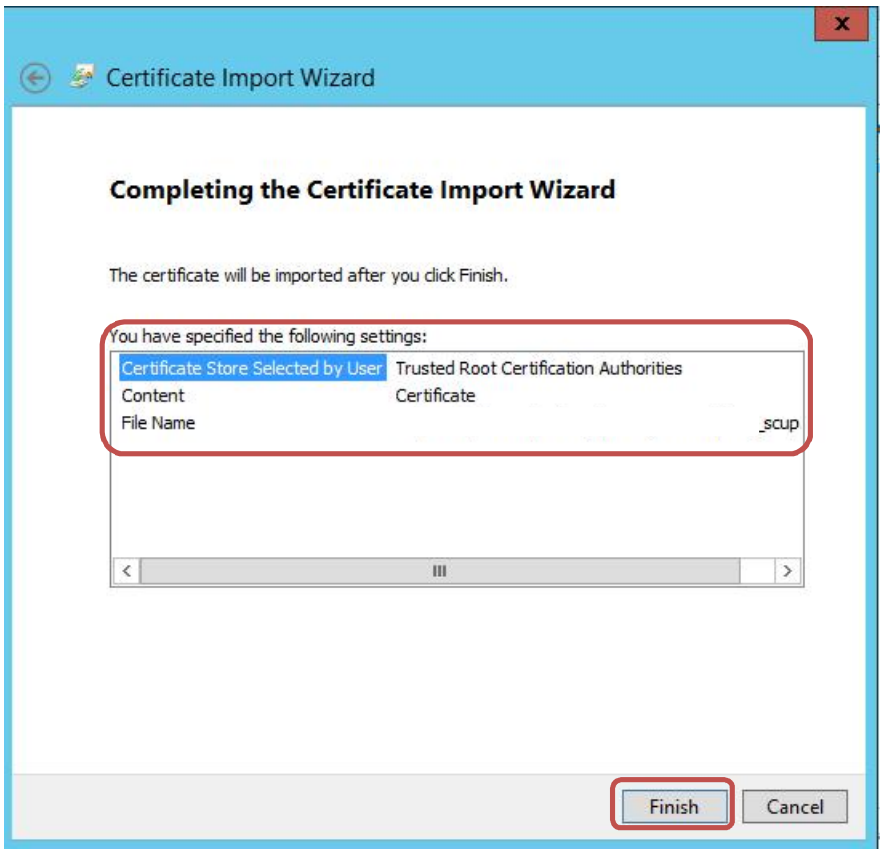
Kuvio 42. Tuotavan varmenteen valinta

Seuraavassa ikkunassa tarkistettiin, että oletus tuontipaikka on oikein ja painettiin ”Next”-painiketta, kuten Kuviossa 43 on esitetty.



Kuvio 43. Varmenteen tuonnin kohde

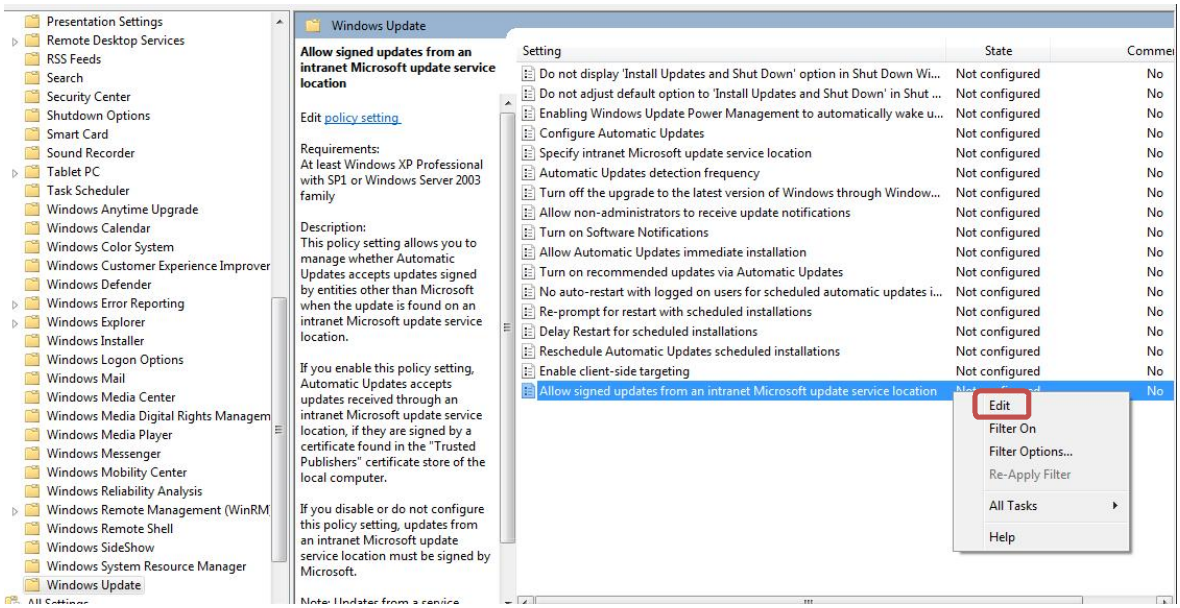
Aukeavasta ikkunasta tarkistettiin, että määritykset ovat oikein ja painettiin ”Finish”-painiketta, kuten kuviossa 44 on esitetty.



Kuvio 44. Tuonnin määritykset

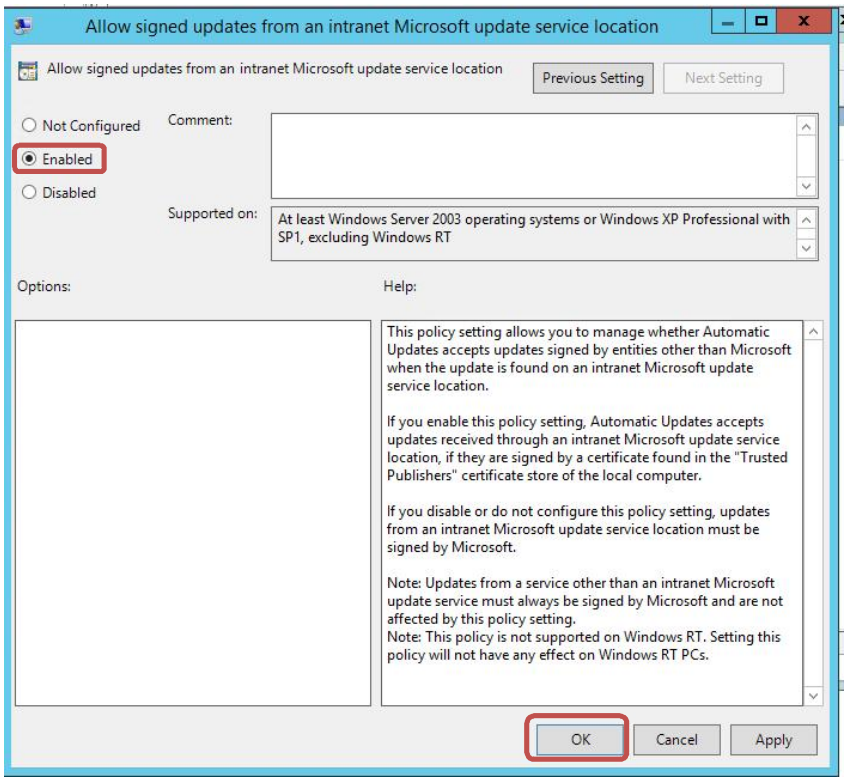
Seuraavaksi samaan GPO:n lisättiin varmenteen tuonti ”Trusted Publisher” -kansioon. Tuonti aloitettiin painamalla hiiren oikealla napilla ”Trusted Publisher” -kansiota ja valitsemalla listasta ”Import…”, kuten kuviossa 40 on esitetty. Kaikki kohdat menivät samalla lailla kuin varmenteen tuonti ”Trusted Root Certification Authorities” -kansioon, ”Trusted Publisher” -kansio löytyy samasta ”Public Key Policies” -kansiosta kuin ”Trusted Root Certification Authorities” -kansio.

Seuraavaksi samaan GPO:n lisättiin määritys, että työasemiin voidaan asentaa allekirjoitettuja päivityksiä sisäverkon päivityspalvelimelta. ”Group Policy Management Editor” -ikkunassa avattiin ”Computer Configuration / Administrative Templates / Windows Components / Windows Update” -kansio ja siellä oikealla hiiren napilla painettiin “Allow signed updates from an intranet Microsoft update service location” -asetusta ja aukeavasta listasta valittiin “Edit”, kuten kuviossa 45 on esitetty.



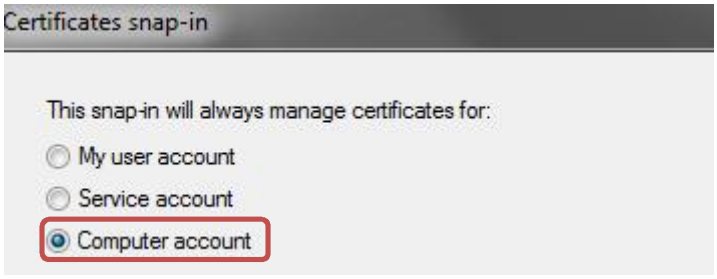
Kuvio 45. Allekirjoitettujen päivitysten asennus sisäverkon palvelimelta

Aukeavasta ikkunasta valittiin määritykseksi ”Enabled” ja painettiin ”OK”-painiketta, kuten kuviossa 46 on esitetty. Tämän jälkeen “Group Policy Management Editor” -ikkuna ja “Group Policy Management” -ikkuna suljettiin. GPO:t leviää työasemille 15 – 30 minuutin kuluessa, riippuen organisaation määrityksistä. Varmenteiden asentaminen työasemille saattaa vaatia työaseman uudelleen käynnistämisen, että varmenteet astuvat voimaan.



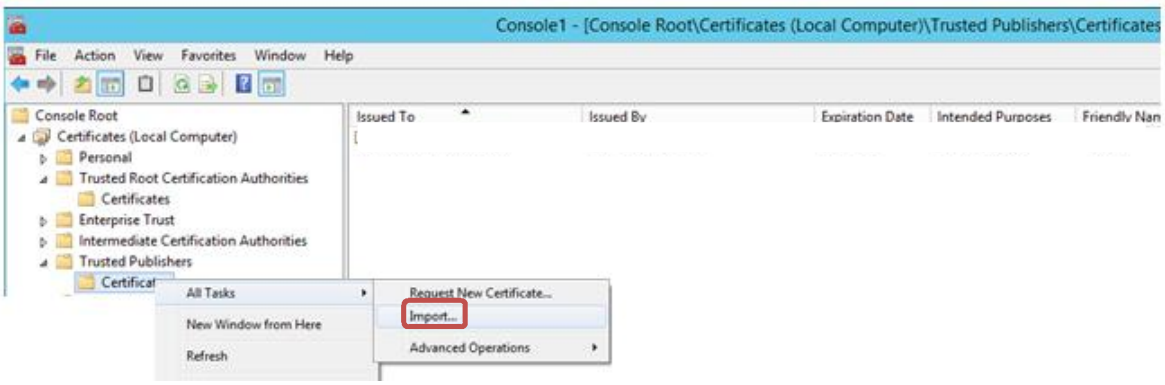
Kuvio 46. GPO määritys

Seuraavaksi varmenne tuotiin WSUS (Windows Server Update Services) -palvelimelle. MMC aukaistiin WSUS palvelimella järjestelmänvalvojana ja siihen lisättiin ”Varmenteet”-laajennus, kuten kuvioissa 15, 16 ja 17 on esitetty, erona kuvioon 17 otettiin asetus tietokonetilistä (Computer Account), kuten kuviossa 47 on esitetty.



Kuvio 47. Tietokonetilin valinta

Aukeavasta ikkunasta avattiin ”Certificates (Local Computer) / Trusted Publisher” -kansio ja painettiin hiiren oikealla napilla ”Certificates”-kansiota ja aukeavasta listasta valittiin ”All tasks / Import…”, kuten kuviossa 48 on esitetty. Sitten varmenteen tuonti meni kuin kuvioissa 41, 42, 43 ja 44, erona, että kuvioissa 43 ja 44 pitää lukea ”Trusted Publisher”, ”Trusted Root Certification Authorities” kohdalla.

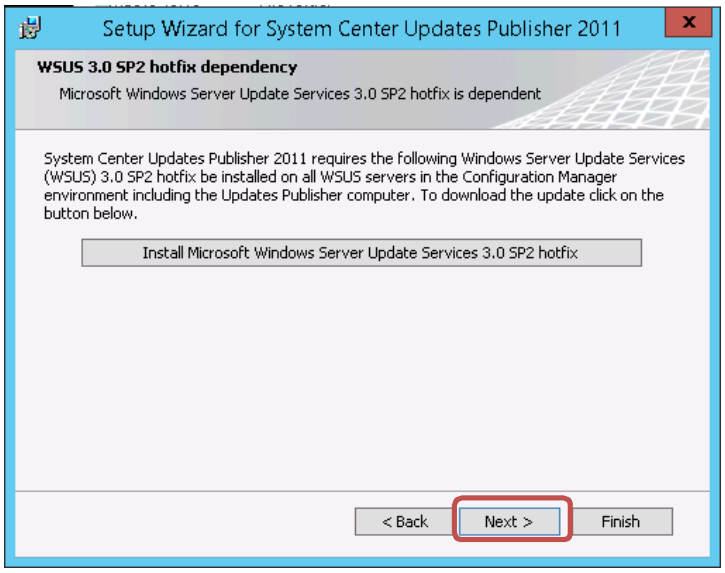


Kuvio 48. Varmenteen tuonti

Seuraavaksi asennettiin SCUP 2011, asennus tehtiin SCCM 2012 CAS:lle (Central Administration Sitel). Asennuksen ensimmäisessä ikkunassa painettiin ”Next >” -painiketta, kuten kuviossa 49 on esitetty.

Kuvio 49. SCUP 2011:n asennuksen aloitus

Seuraavassa ikkunassa asennus pyytää asentamaan Service Pack 2 päivityksen WSUS versioon 3, testiympäristössä oli käytössä WSUS versio 4 joten päivitystä ei tarvinnut asentaa ja ikkunassa painettiin ”Next >” -painiketta, kuten kuviossa 50 on esitetty.

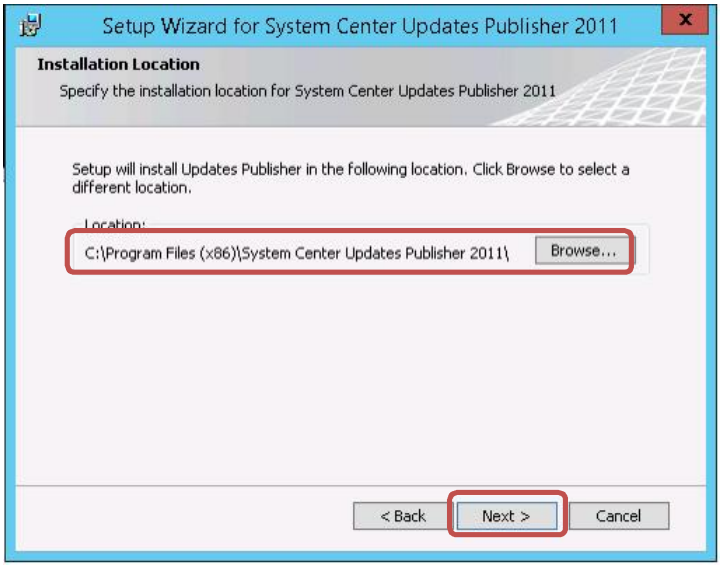


Kuvio 50. Service Pack 2 asennus WSUS versio 3

Seuraavassa ikkunassa valittiin ”I accept the licence agreement” ja painettiin ”Next >” -painiketta, kuten kuviossa 51 on esitetty.

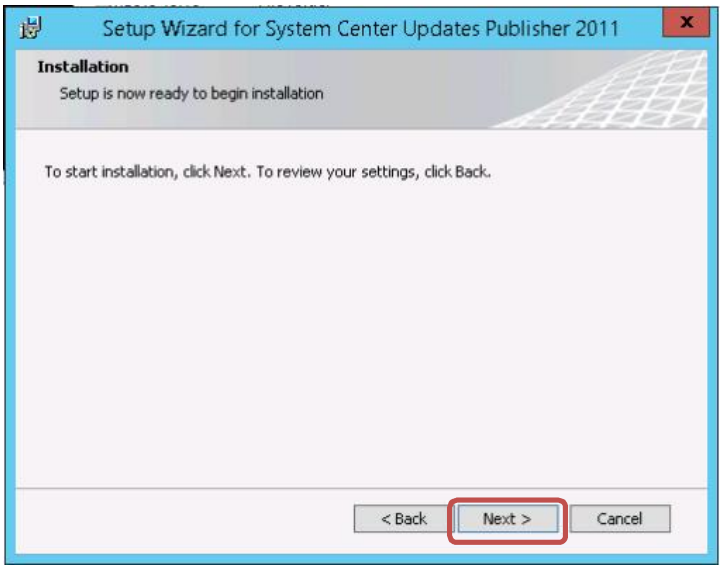
Kuvio 51. Lisenssiehtojen hyväksyntä

Seuraavassa ikkunassa valittiin asennuksen kohdekansio ja painettiin ”Next >” -painiketta, kuten kuviossa 52 on esitetty.



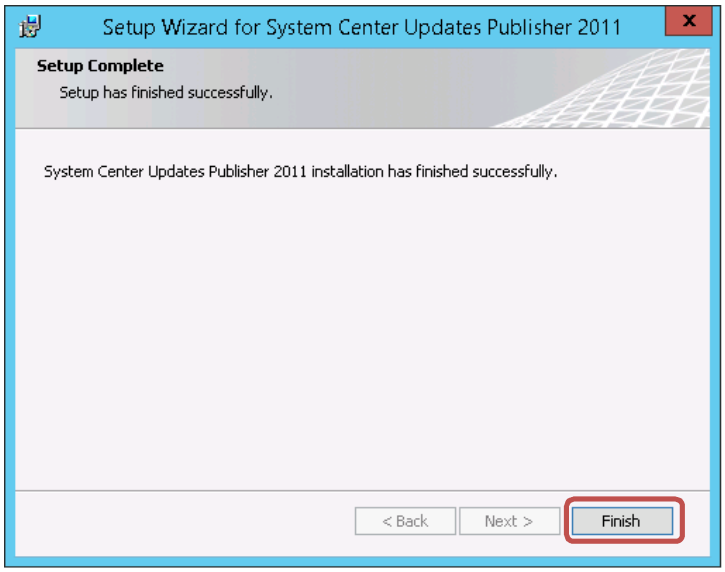
Kuvio 52. Asennuskansion valinta

Seuraavassa ikkunassa asennus aloitettiin painamalla ”Next >” -painiketta, kuten kuviossa 53 on esitetty.



Kuvio 53. Asennuksen aloitus

Seuraavassa ikkunassa painettiin ”Finish”-painiketta, kuten kuviossa 54 on esitetty.

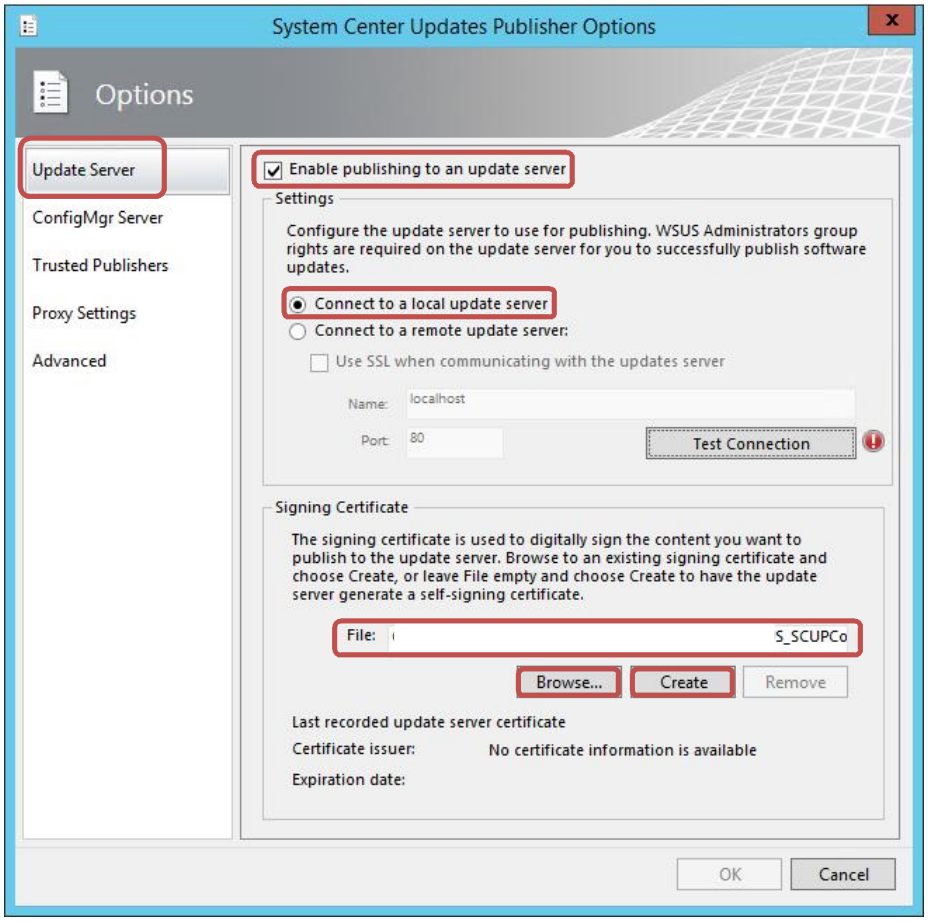


Kuvio 54. Asennukset viimeistely

Seuraavaksi määritettiin SCUP 2011 -asetukset, SCUP 2011 aukaistiin järjestelmänvalvojan oikeuksilla ja vasemman ylänurkan listasta painettiin ”Options”-painiketta, kuten kuviossa 55 on esitetty.

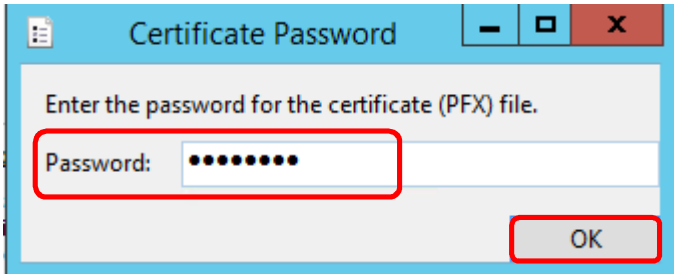
Kuvio 55. Asetusten määrittämisen aloitus

Seuraavassa ikkunassa ”Update Server” -kohdasta valittiin ”Enable publishing to an update server” ja ”Connect to a local update server” sekä “Signing Certificate” -kohdasta “Browse…” -painikkeesta aukeavasta ikkunasta haettiin kuvioissa 31-36 luotu ”.pfx” -päätteinen allekirjoitusvarmenne, kun varmenteen sijainti oli määritetty, painettiin ”Create” -painiketta, kuten kuviossa 56 on esitetty.



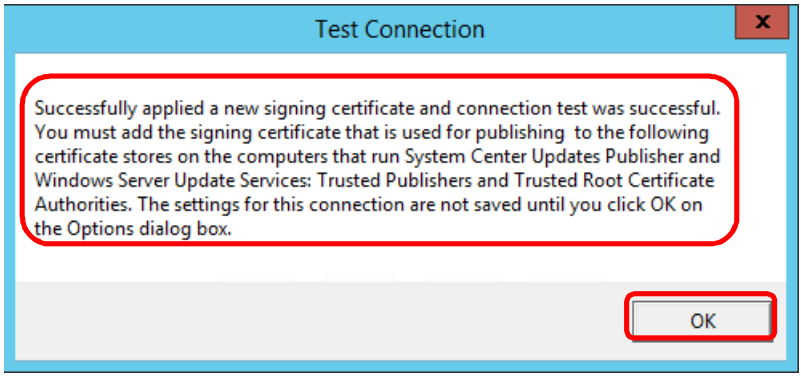
Kuvio 56. Päivityspalvelimen asetukset

Seuraavassa ikkunassa annettiin varmenteen salasana, mikä varmenteelle määritettiin luonnin yhteydessä ja painettiin ”OK”-painiketta, kuten kuviossa 57 on esitetty.



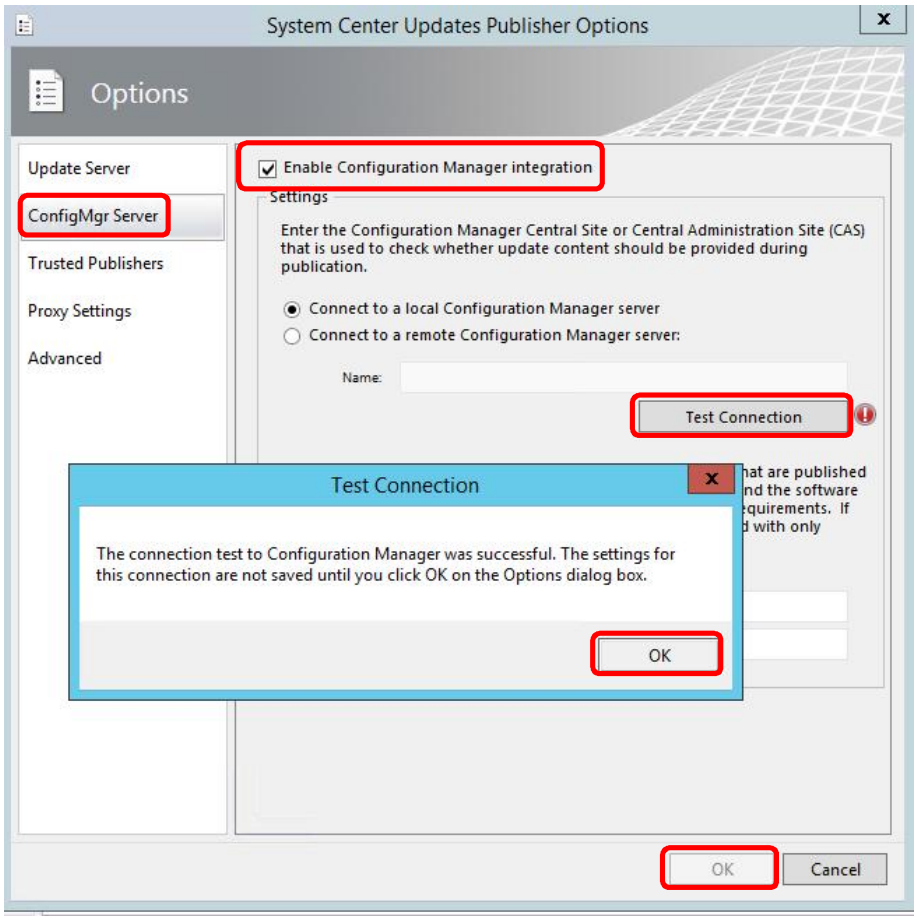
Kuvio 57. Varmenteen salasana

Seuraavaksi SCUP 2011 lisää allekirjoitusvarmenteen ja testaa yhteyden päivityspalvelimeen automaattisesti, ikkunassa painettiin ”OK”-painiketta, kuten kuviossa 58 on esitetty.



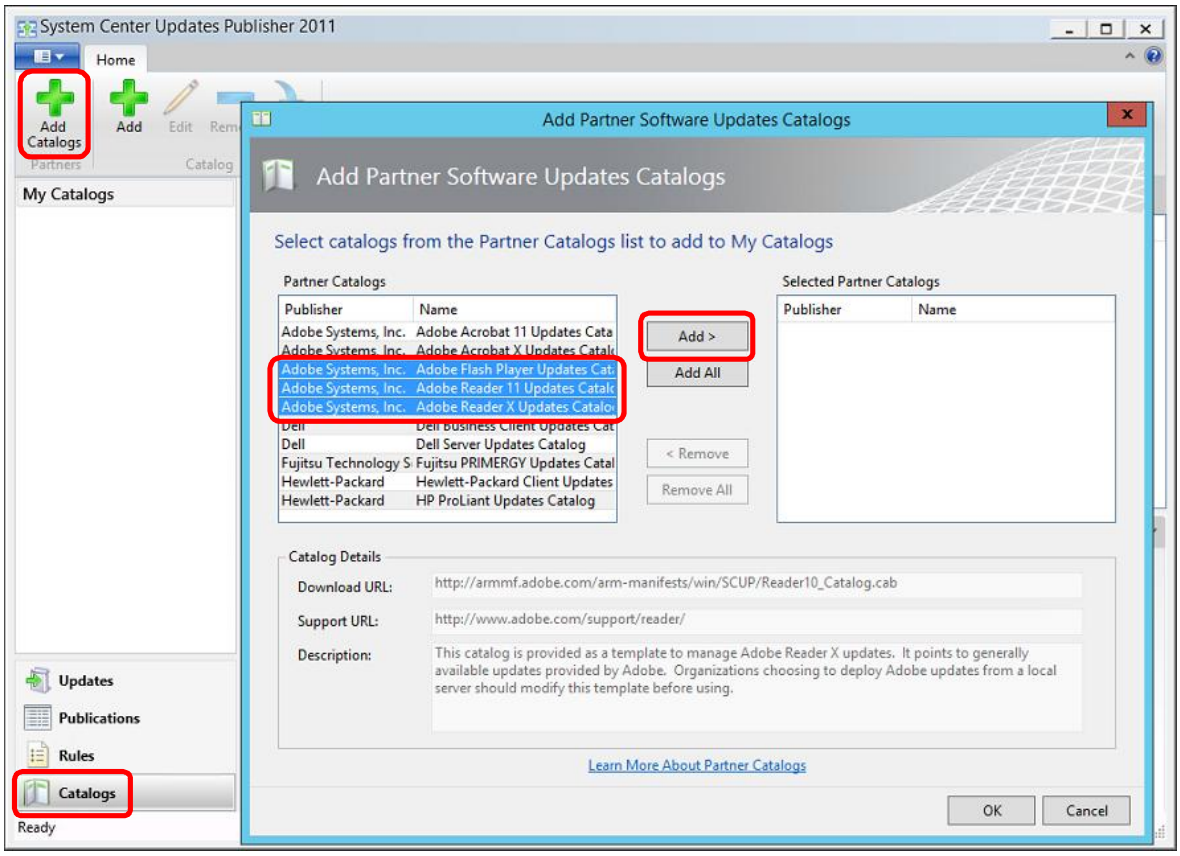
Kuvio 58. Yhteyden testaus päivityspalvelimeen

Seuraavaksi valittiin ”ConfigMgr Server” -välilehti ja valittiin asetuksiksi ”Enable Configuration Manager integration” ja ”Connect to a local Configuration Manager server” sekä painettiin ”Test Connection” -painiketta. Aukeavasta ikkunasta painettiin “OK”-painiketta ja tämän jälkeen asetusikkuna suljettiin painamalla “OK”-painiketta, kuten kuviossa 59 on esitetty.



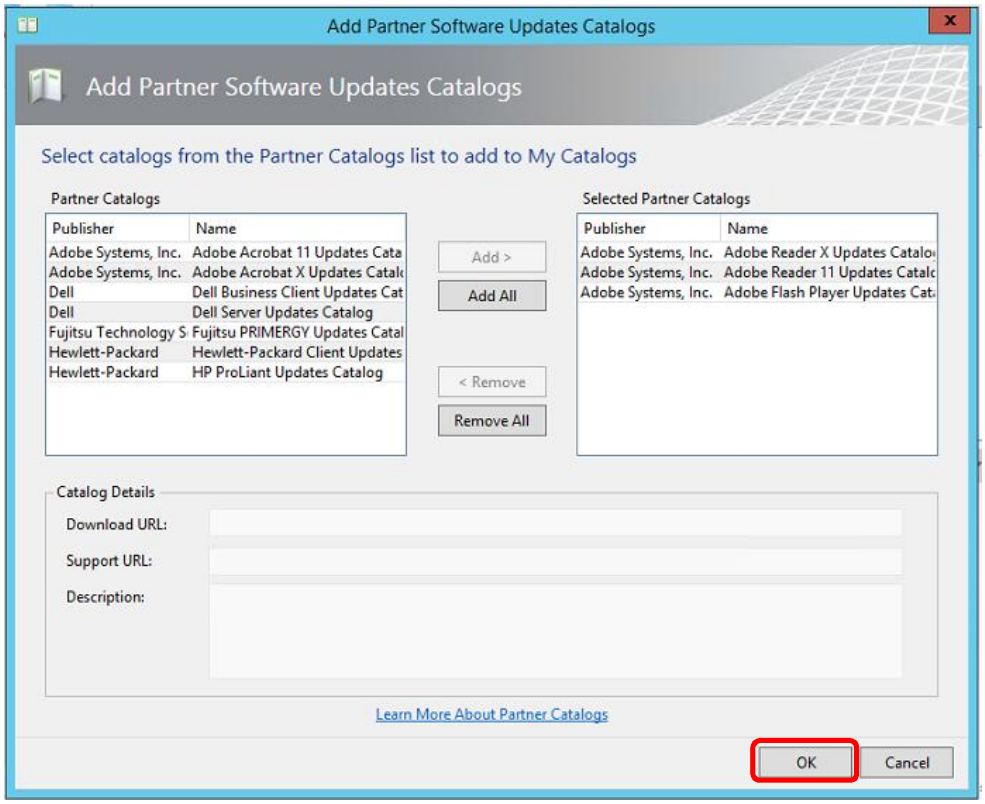
Kuvio 59. Yhteyden määritys SCCM 2012:n

Seuraavaksi SCUP 2011:n lisättiin Adobe Acrobat Readerin ja Adobe Flash Playerin käytössä olevien versioiden päivitysluettelot. Ensin valittiin ”Catalogs” -välilehti ja sieltä painettiin ”Add Catalogs” -painiketta. Aukeavasta ikkunasta valittiin päivitysluettelot ja painettiin ”Add >” –painiketta, kuten kuviossa 60 on esitetty.



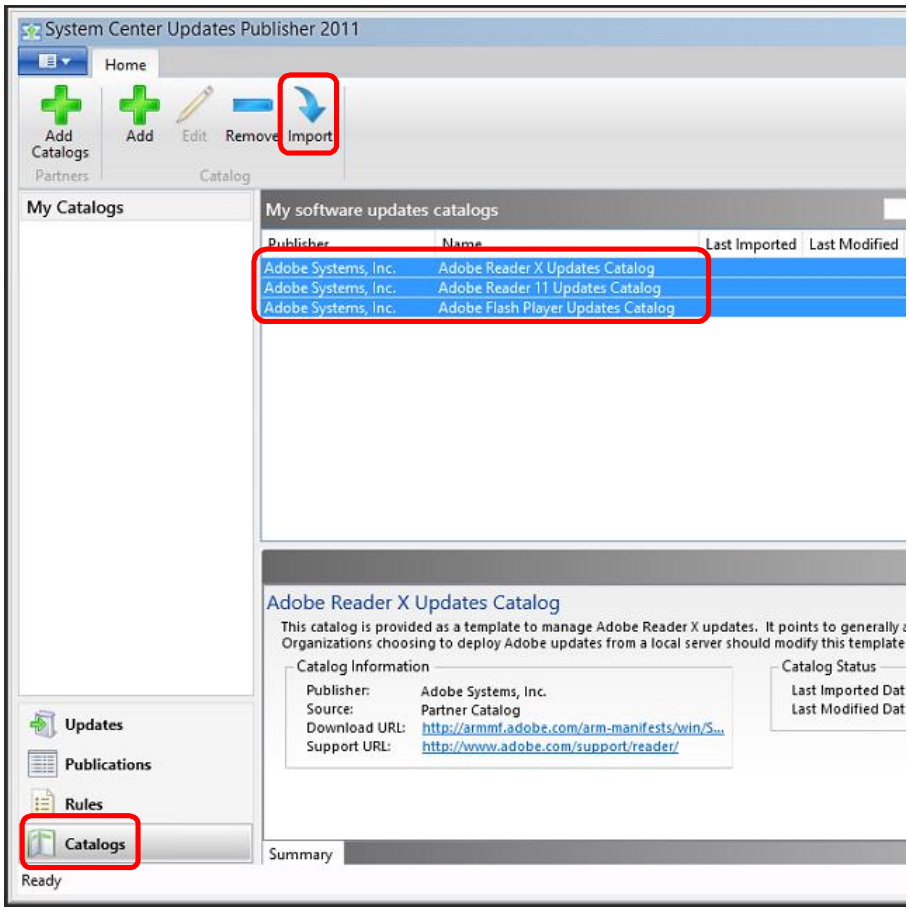
Kuvio 60. Päivitysluetteloiden lisääminen

Seuraavaksi, kun päivitysluettelot oli valittu, painettiin ”OK”-painiketta, kuten kuviossa 61 on esitetty.



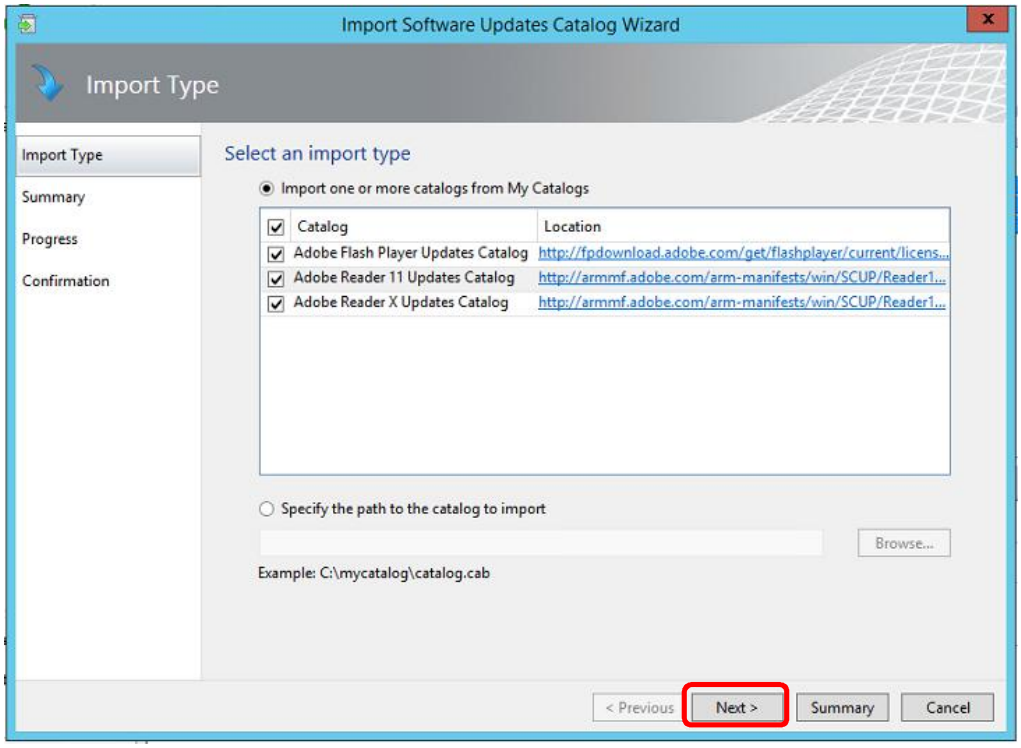
Kuvio 61. Päivitysluetteloiden lisäyksen viimeistely.

Seuraavaksi ”Catalogs”-välilehdellä päivitysluetteloihin haettiin päivitykset, valitsemalla päivitykset ja painamalla ”Import”-painiketta, kuten kuviossa 62 on tehty.



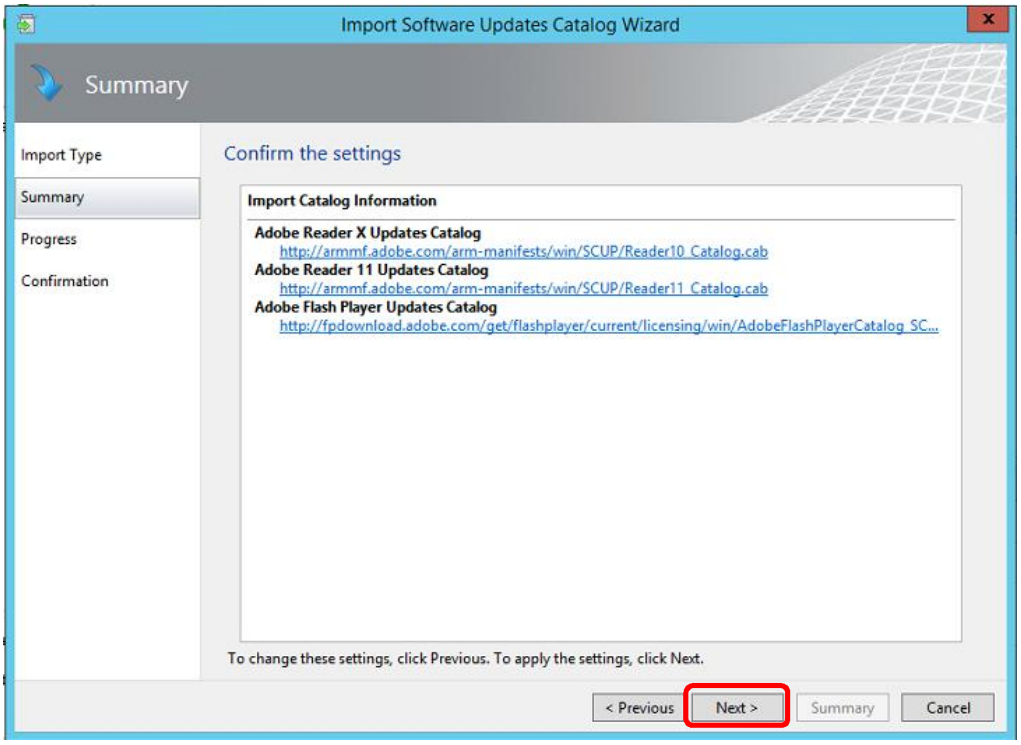
Kuvio 62. Päivitysten tuonti päivitysluetteloihin

Seuraavassa ikkunassa painettiin ”Next >” -painiketta, kuten kuviossa 63 on esitetty.



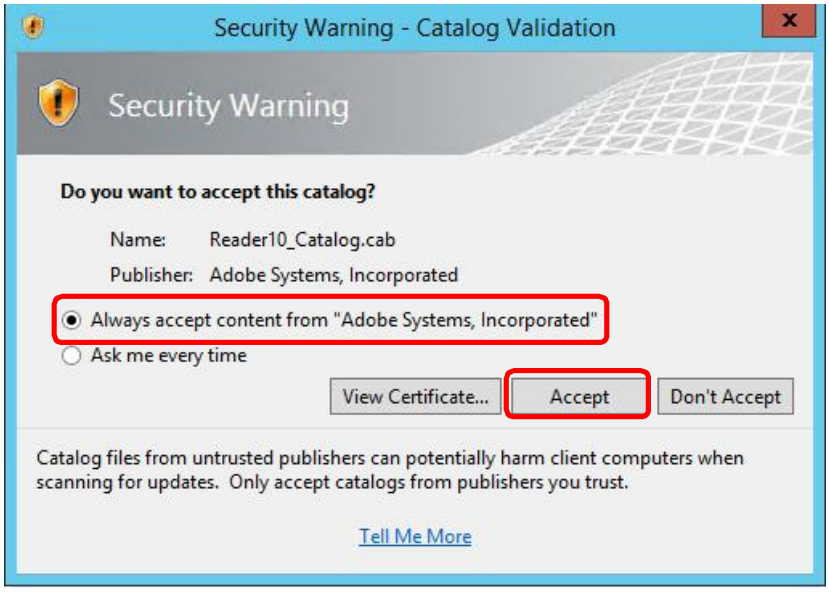
Kuvio 62. Päivitysten tuonti

Seuraavassa ikkunassa painettiin ”Next >” -painiketta, kuten kuviossa 63 on esitetty.



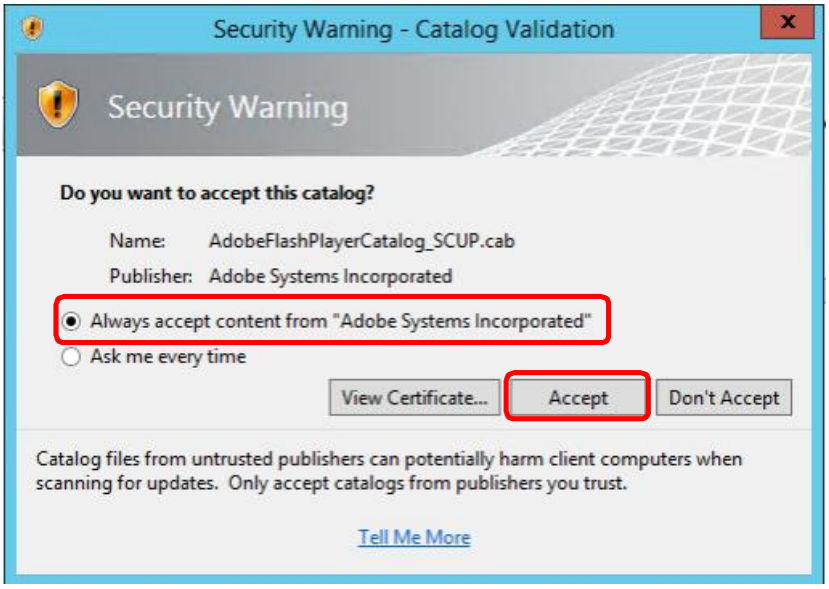
Kuvio 63. Päivitysten tuonnin viimeistely

Seuraavaksi päivitysluetteloiden asennukset antoivat suojausvaroituksen. Suojausvaroituksiin valittiin ”Always accept content from ”Adobe Systems, Incorporated” -asetus ja painettiin ”Accept”-painiketta, kuten kuvioissa 64, 65 ja 66 on esitetty.



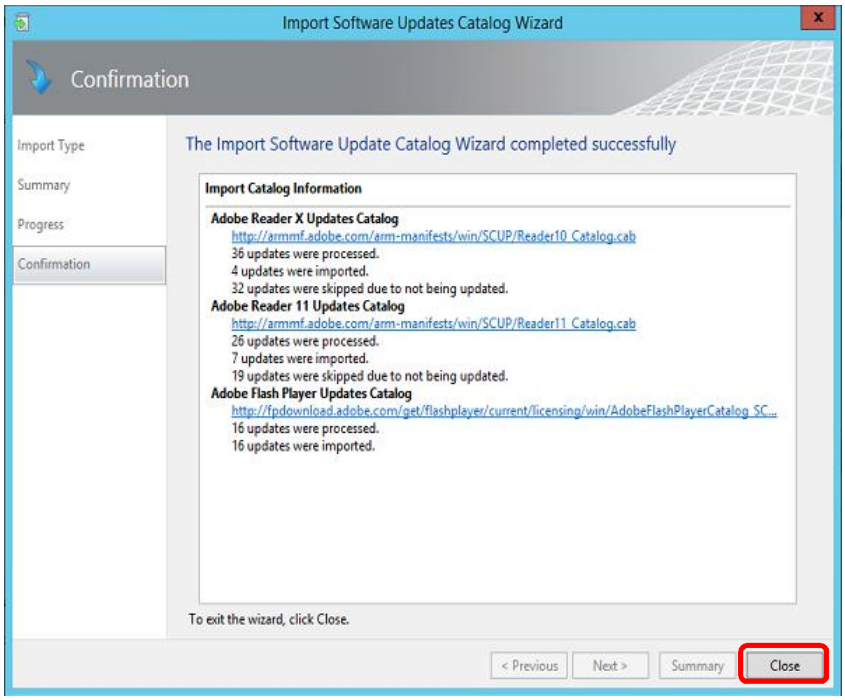
Kuvio 64. ”Reader 10” -päivitysluettelon suojausvaroituksen hyväksyminen

Kuvio 65. ”Reader 11” -päivitysluettelon suojausvaroituksen hyväksyminen



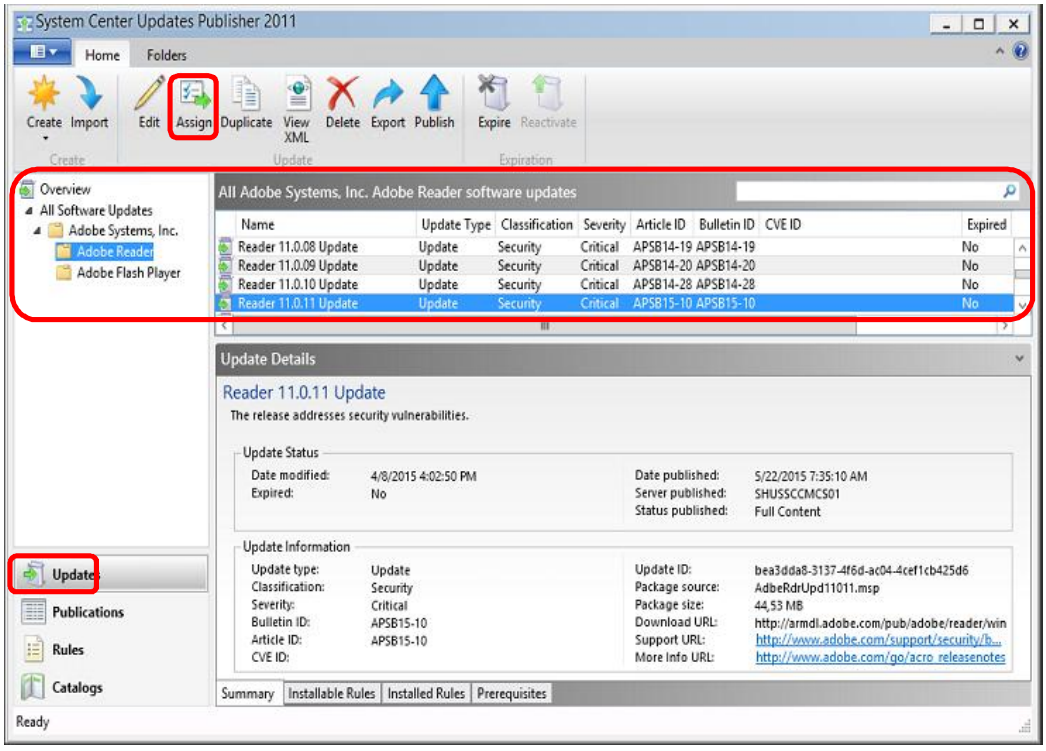
Kuvio 66. ”Flash Player” -päivitysluettelon suojausvaroituksen hyväksyminen

Seuraavassa ikkunassa painettiin ”Close”-painiketta, kuten kuviossa 67 on esitetty.



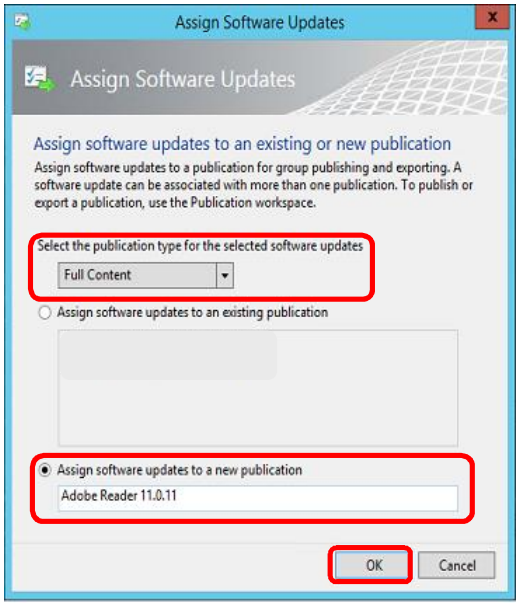
Kuvio 67. Päivitysluettelon tuonnin viimeistely

Seuraavaksi halutuista päivityksistä tehtiin julkaisupaketti ja se julkaistiin SCCM 2012:sta, tässä projektissa julkaisua ja päivitystä testattiin ”Adobe Acrobat Reader 11” -versiolla. SCUP 2011:sta ikkunassa valittiin ”Updates”-välilehti ja päivityksistä valittiin haluttu päivitys ja painettiin ”Assign”-painiketta, kuten kuviossa 68 on esitetty.



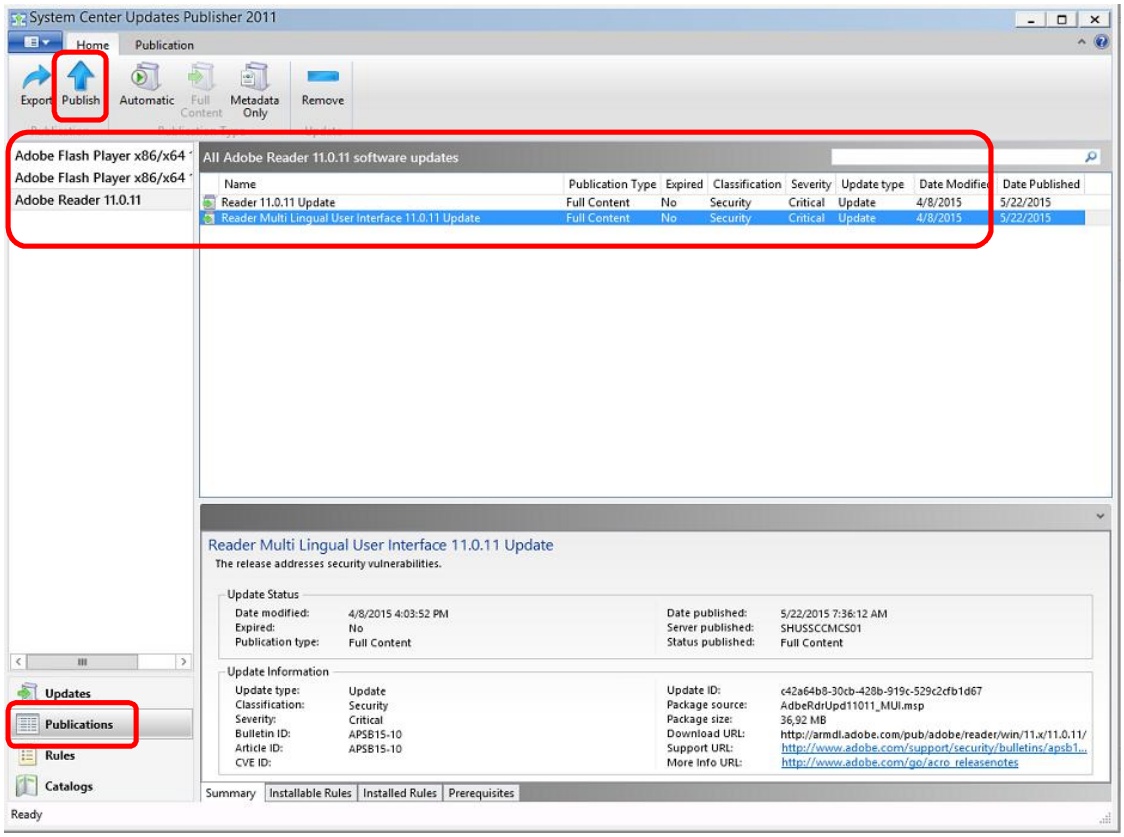
Kuvio 68. Julkaisupaketin luonnin aloitus

Aukeavassa ikkunassa valittiin ”Select the publication type for the selected software updates” -pudotusvalikosta ”Full Content”, julkaisupaketille annettiin nimi ”Assign software updates to a new publication” kohtaan ja painettiin “OK”-painiketta, kuten kuviossa 69 on esitetty.



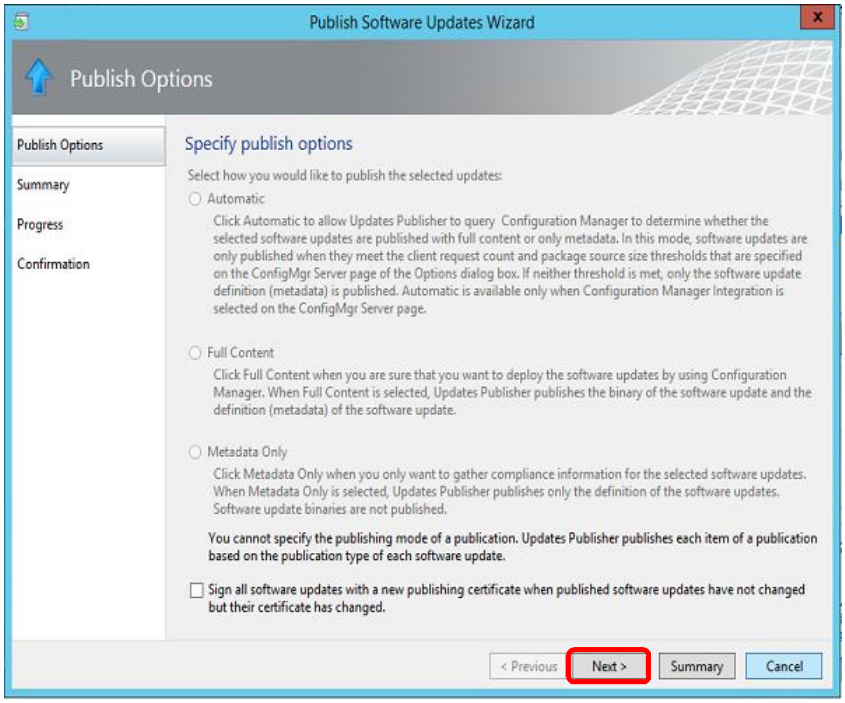
Kuvio 69. Julkaisupaketin määritys

Seuraavaksi julkaisupaketti julkaistiin, SCUP 2011:n pääikkunasta valittiin ”Publications”-välilehti ja valittiin julkaistava päivitys, lopuksi painettiin ”Publish”-painiketta, kuten kuviossa 70 on esitetty.



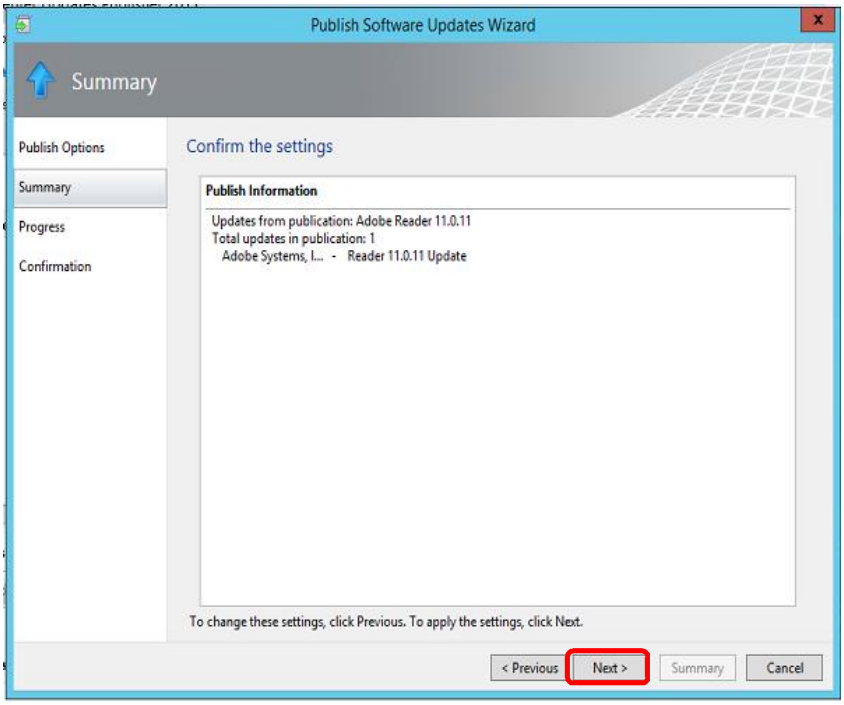
Kuvio 70. Julkaisupaketin julkaisu

Aukeavassa ikkunassa painettiin ”Next >” -painiketta, kuten kuviossa 71 on esitetty.



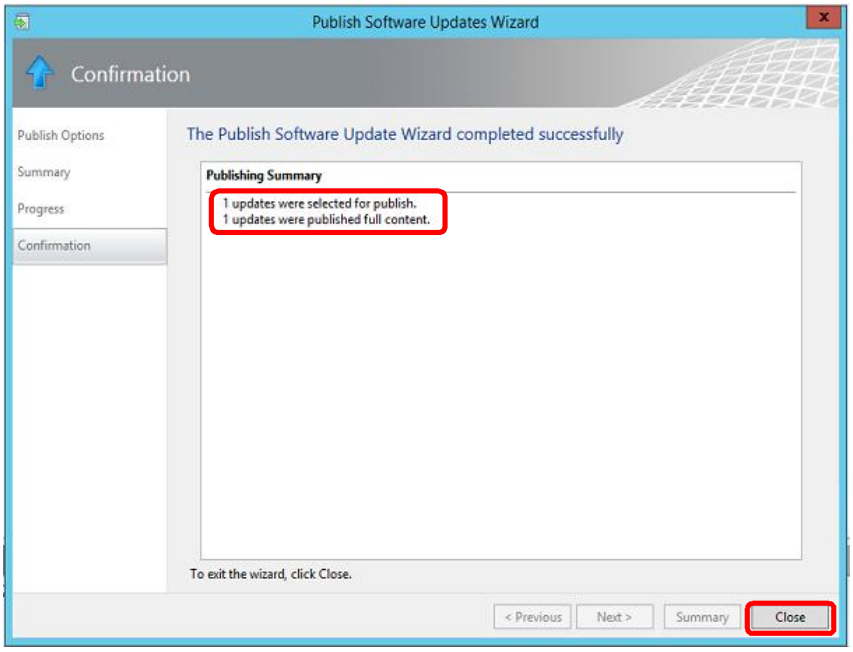
Kuvio 71. Julkaisun aloitus

Seuraavassa ikkunassa painettiin ”Next >” -painiketta, kuten kuviossa 72 on esitetty.



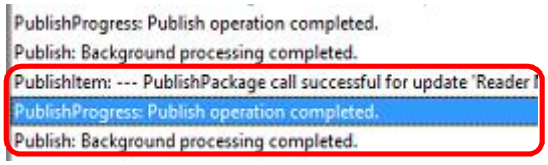
Kuvio 72. Julkaisun tiedot

Seuraavassa ikkunassa painettiin ”Close”-painiketta, kuten kuviossa 72 on esitetty.



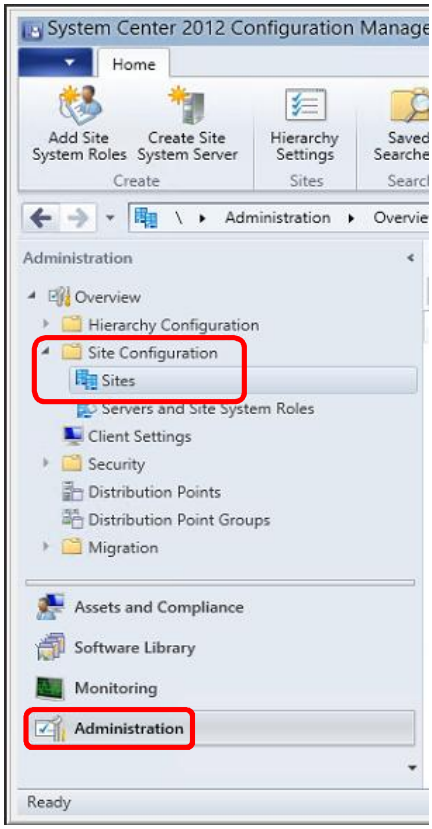
Kuvio 73. Julkaisun viimeistely

Seuraavaksi tarkistettiin kirjaustiedostosta, että julkaisu onnistui. Kirjaustiedosto on ”SCUP.log” -niminen ja se sijaitsee ”C:\Users\%username%\AppData\Local\Temp\” -hakemistossa, tiedostosta etsittiin julkaistava paketin nimi ja että se onnistui, kuten kuviossa 73 on esitetty.



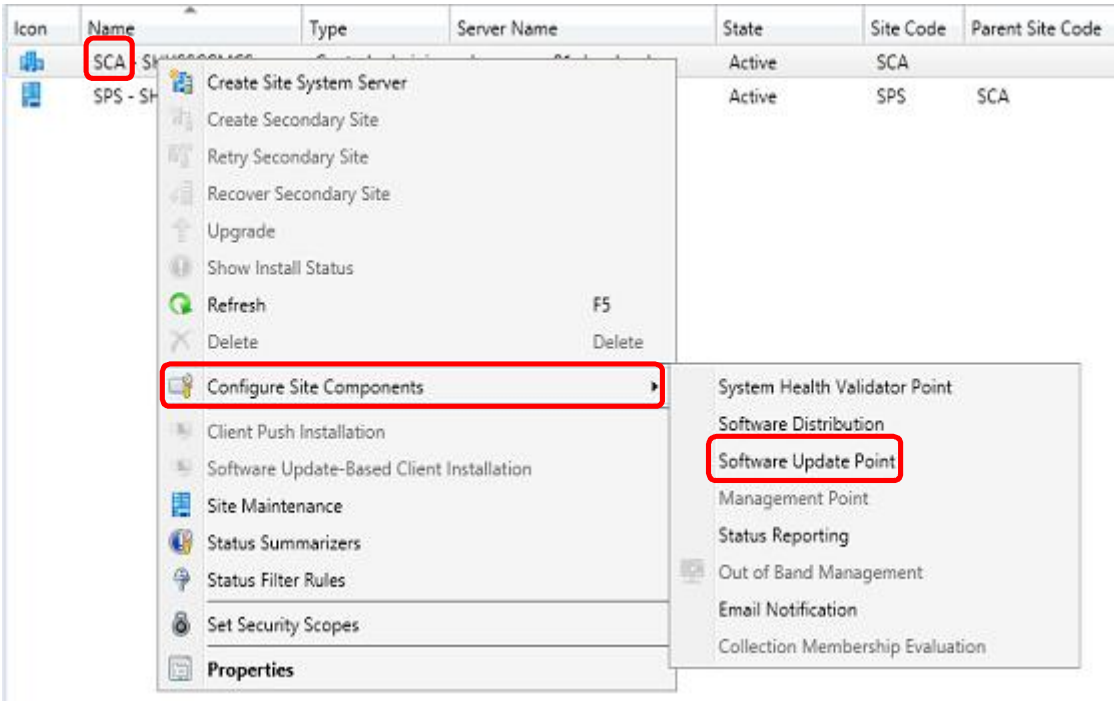
Kuvio 73. Julkaisun onnistumisen tarkistaminen

Seuraavaksi määritettiin SCCM 2012:n päivityspisteeseen haetaan ”Adoben Flash Player” ja ”Adobe Reader” -päivitykset. SCCM 2012:n hallintaikkunasta valittiin ”Administration”-välilehti ja ”Site Configuration” -kansion alta painettiin ”Sites”-painiketta, kuten kuviossa 74 on esitetty.



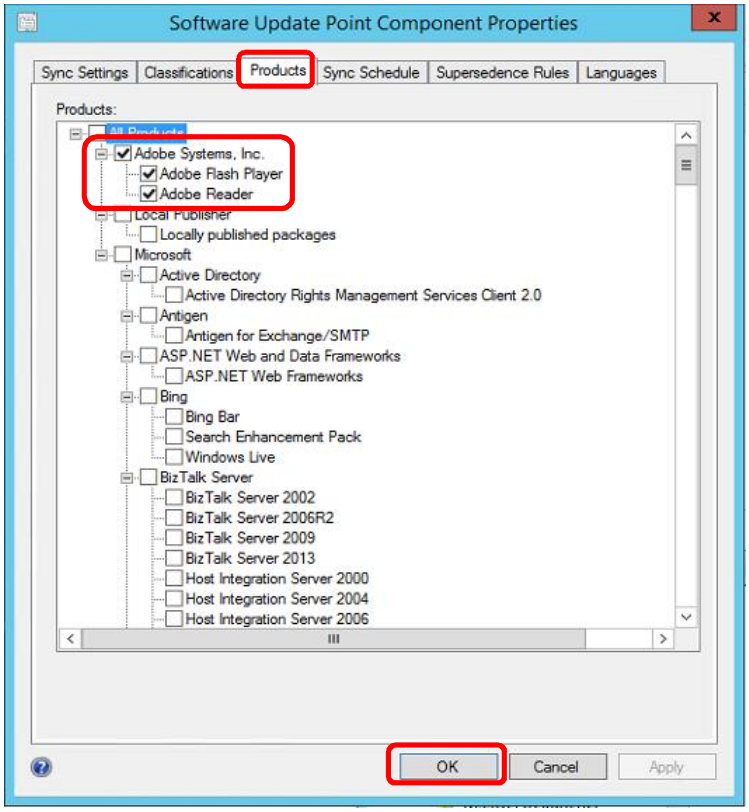
Kuvio 74. SCCM 2012:n määritys

Seuraavaksi painettiin hiiren oikealla painikkeella CAS:n päällä ja valittiin ”Configure Site Components” -valikosta ”Software Update Point”, kuten kuviossa 75 on esitetty.



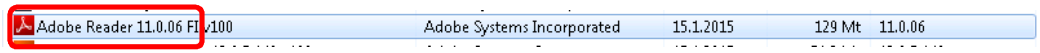
Kuvio 75. SCCM:n päivityspisteen määrittäminen

Seuraavasta ikkunasta aktivoitiin ”Products”-välilehti ja sieltä valittiin ”Adobe Flash Player” ja ”Adobe Reader” -tuotteet, lopuksi painettiin ”OK”-painiketta, kuten kuviossa 76. on esitetty.



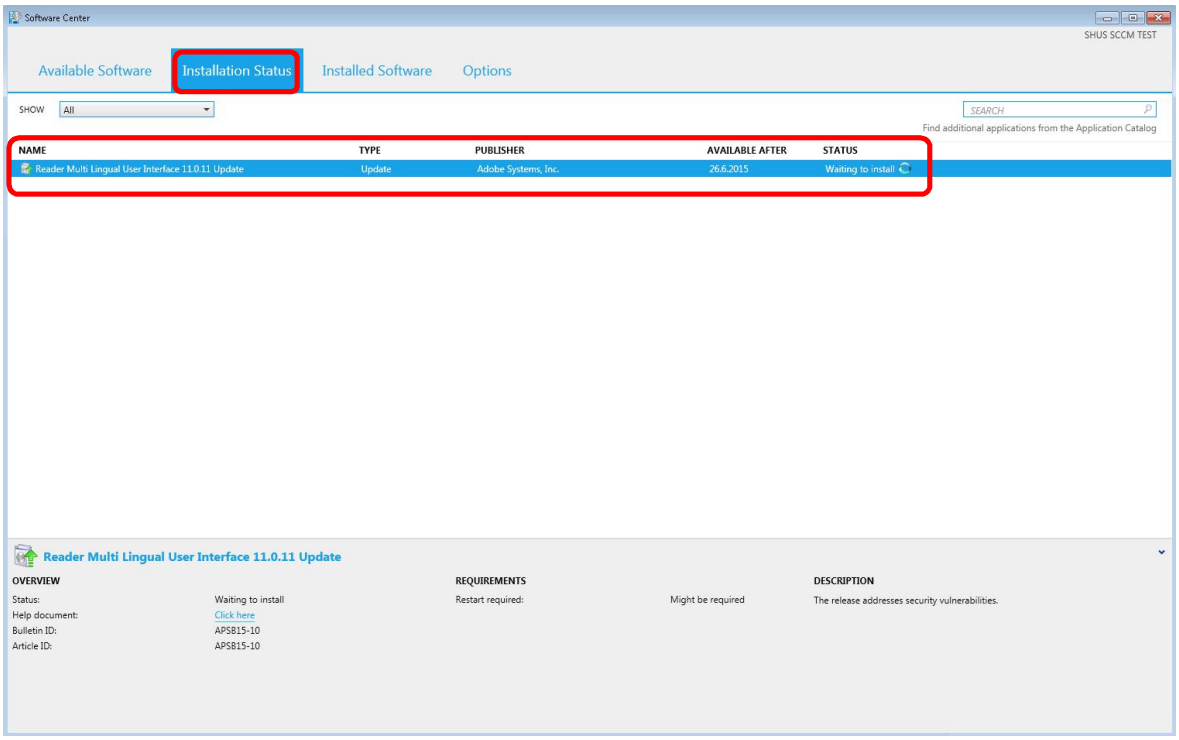
Kuvio 76. Adobe tuotteiden valinta

Seuraavaksi ”Adobe Reader” -päivitykset levitettiin SCCM 2012:lla testityöasemille, SCCM 2012:n operointi on rajattu pois projektin sisällöstä. Ennen levitystä tarkistettiin testityöaseman asennetuista sovelluksista ”Adobe Reader” -versio, kuten kuviossa 77 on esitetty.

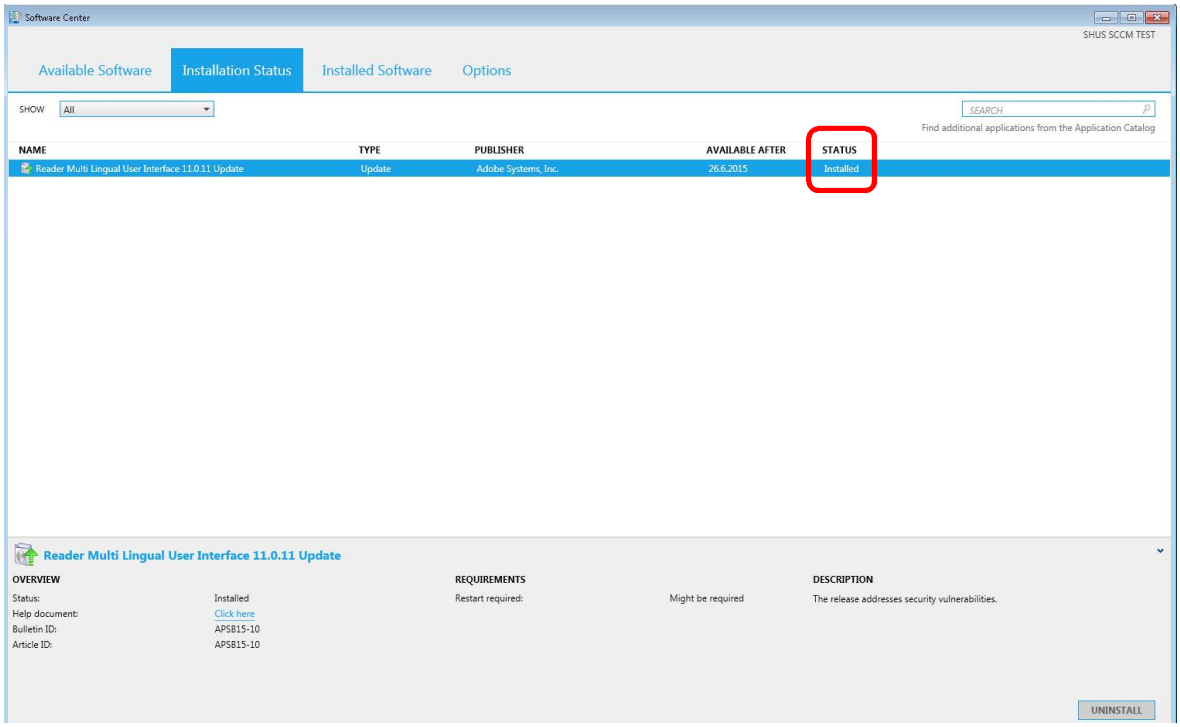


Kuvio 77. Adobe Readerin version tarkistaminen

Kun päivityksen levitys oli käynnistetty testityöasemalle, tarkistettiin testityöaseman ”Software Center” -ohjelman ”Installation Status” -välilehdeltä, että asennus käynnistyi ja valmistui, kuten kuvioissa 78 ja 79 on esitetty.

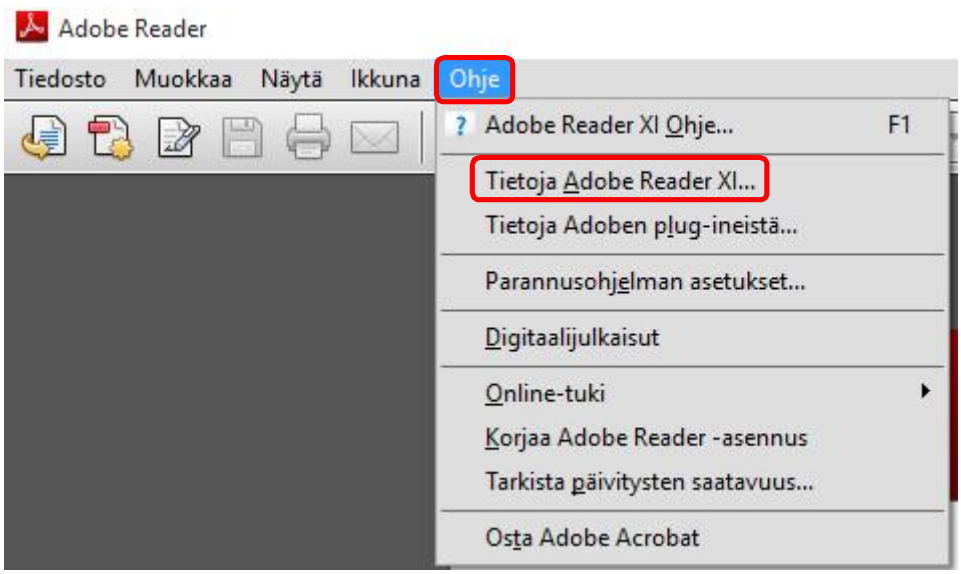


Kuvio 78. Päivityksen asennuksen aloituksen tarkistaminen



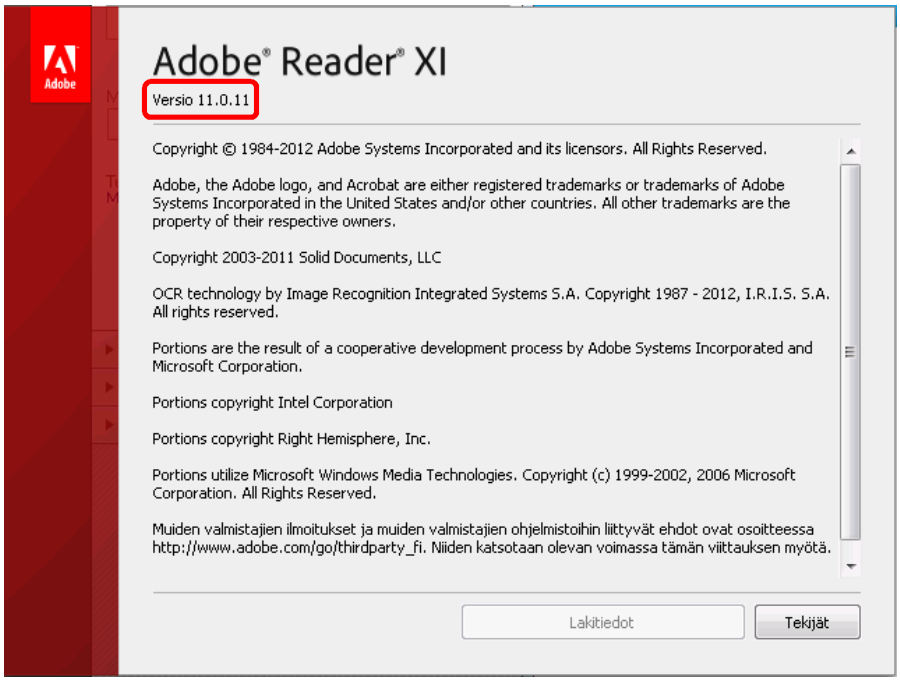
Kuvio 79. Päivityksen asennuksen valmistumisen tarkistaminen

Lopuksi avattiin ”Adobe Reader XI” -ohjelma ja sen ”Ohje”-valikon alta valittiin ”Tietoja Adobe Reader XI…” -valinta, kuten kuviossa 80 on esitetty.



Kuvio 80. ”Adobe Readerin Ohje” -valikko

Avautuvasta ikkunasta tarkistettiin, että versio on päivittynyt, kuten kuvio 81 on esitetty.



Kuvio 81. Adobe Reader version tarkistaminen

4.3 Tulokset

Tuloksena oli asennettu SCUP 2011 -työkalu testiympäristöön. SCUP 2011:n käyttöönotto vaiheittain: ensin tehdään allekirjoitus varmennepohja ja julkaistaan varmennepohja. Haetaan ja tallennetaan varmenne toimialueella olevaan työasemaan. Haetaan ja tallennetaan varmenteen yksityisavain (Private Key) toimialueella olevaan työasemaan. Luodaan GPO varmenteen levitystä varten, jolla tuodaan varmenne työaseman Trusted Root Certification Authorities ja Trusted Publisher -kansioihin. Tähän GPO:n laitetaan myös määritys, että allekirjoitetut päivitykset ovat luotettuja asentaa sisäverkosta. Tuodaan varmenne WSUS-palvelimen Trusted Publishers -kansioon. Asennetaan SCUP 2011, määritetään SCUP 2011:n asetukset ja testataan yhteyden toiminta SCCM 2012:n kanssa. Tehdään julkaisupaketti, haetaan siihen julkaistavat päivitykset ja julkaistaan paketti. Määritetään SCCM 2012:n software update pointille julkaistujen päivitysten haku. Tehdään päivityksen levitys SCCM 2012:sta ja tarkistetaan työasemalta päivityksen onnistuminen.

5 Päätelmät

Opinnäytetyön tavoitteena oli saada SCUP 2011 -työkalun käyttöönottosuunnitelma tuotantoympäristöön. Tutkimuskysymyksinä opinnäytetyölle oli, että mitä on tieto- ja kyberturvallisuus, mikä on SCUP 2011, miten SCUP 2011 toimii, mitä hyötyä SCUP 2011 -työkalun käytöstä on ja miten SCUP 2011 -työkalu otetaan käyttöön?

Mitä on tieto- ja kyberturvallisuus? Tieto- ja kyberturvallisuus on järjestelyitä, joilla pyritään turvaamaan organisaation it-ympäristön ja tietojen käytettävyys, eheys ja luottamuksellisuus erilaisissa uhkatilanteissa.

Mikä on SCUP 2011? SCUP 2011 on työkalu, millä voidaan julkaista muiden ohjelmistovalmistajien kuin Microsoftin sovellusten päivityksiä WSUS -päivityspalvelimelle, mistä ne voidaan levittää organisaation työasemille SCCM 2012 -järjestelmällä.

Miten SCUP 2011 toimii? SCUP 2011 -työkalulla voi julkaista valmiita sovelluspäivityskatalogeja tai luoda omia päivityskatalogeja, sovelluksista jotka ovat ladattavissa internetistä.

Mitä hyötyä SCUP 2011 -järjestelmän käytöstä on? SCUP 2011 -työkalulla julkaistut ohjelmistopäivitykset, voidaan asentaa työasemille tietoturvapäivityksinä, eivätkä asennukset näy käyttäjille häiritsevinä asennusikkunoina.

Miten SCUP 2011 -työkalu otetaan käyttöön? SCUP 2011 -työkalun käyttöönottoon kuuluu erilaisia työvaiheita muun muassa allekirjoitusvarmenteen luonti ja jakelu työasemille GPO:n avulla. Ilman varmennetta ei SCUP 2011 -työkalun määritystä voi suorittaa onnistuneesti. Määrityksien jälkeen luodaan päivityspaketti mikä julkaistaan WSUS-palvelimelle ja sieltä se haetaan ja levitetään SCCM 2012 -järjestelmällä työasemille.

Mielestäni onnistuin hyvin tavoitteiden saavuttamisessa. Käyttöönottosuunnitelman avulla tehtiin tuotantokäyttöönotto onnistuneesti. Testiympäristössä ilmentyneiden ongelmien korjauksiin menneen ajan takia suunniteltu aikataulu venähti vähän, mutta ei mitenkään radikaalisti.

Kirjoittamisen alussa meinasi seinä nousta vastaan, kun aloitin kirjoittamisen ohjelmistojen tietoturvan päivittämisestä, enkä löytänyt lähdemateriaalia mistään, siis näin tietojärjestelmäinfrastruktuurin ylläpidon näkökulmasta. Jonkun verran asiasta löytyi ohjelmistokehittäjien tutkielmia parhaista tavoista nostaa ohjelmistojen tietoturvaa niin kehittämis- että

ylläpitovaiheessa. Lopulta kirjoitin syistä, että miksi tietoturvapäivitysten asennuksen jatkuvahallinta on elintärkeää, eli kyberuhista, haavoittuvuuksista ja käsitteistä mitä liittyy tieto- ja kyberturvallisuuteen.

Työtä tehdessä kehityin ammatillisesti Windows Server -käyttöjärjestelmän ylläpidossa, SCCM 2012 -järjestelmän operoinnissa ja määrittämisessä. Opin asentamaan ja määrittämään SCUP 2011 -työkalun ja julkaisemaan sillä päivityspaketteja. Tietoa etsiessä, löysin paljon tietoa erilaisista uhkista, joita it-ympäristöihin kohdistuu ja mistä tietoa voi tulevaisuudessakin etsiä.

Pilotoinnin ollessa yksi tärkeimmistä seikoista sovelluspäivityksiä tehtäessä. Jatkossa kannattaa jatkuvasti ylläpitää ja kerätä lisää sovellustestaajia sovelluspäivitysten pilottiryhmään. Lisäksi kannattaa luoda uusia päivityskatalogeja tietyille kolmannen osapuolen sovelluksille ja määrittää niille testaajat pilottiryhmään.

Lähteet

ENISA 2016. ENISA threat landscape 2015. European Union Agency for Network and Information Security. Luettavissa: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015/etl2015/at_download/fullReport. Luettu: 2.3.2016.

FIRST 2015. Common Vulnerability Scoring System v3.0. The Forum of Incident Response and Security Team. First.org, Inc. Luettavissa: https://www.first.org/cvss/cvss-v30-specification-v1.7.pdf. Luettu: 15.3.2016.

Järvinen, P. 2002. Tietoturva & yksityisyys. Docendo. Jyväskylä.

Limnéll, J., Majewski, K., Salminen, M. & Samani, R. 2015. Cyber Security for decision makers. Docendo. Jyväskylä.

Microsoft 2011a. Microsoft Security Update Guide, Second Edition. Luettavissa: https://technet.microsoft.com/en-US/security/dn550891. Luettu: 12.3.2016.

Microsoft 2011b. Updates Publisher 2011. Luettavissa: https://technet.microsoft.com/en-us/library/hh134742.aspx. Luettu: 21.3.2016.

Microsoft 2015. Microsoft System Center. Luettavissa: https://technet.microsoft.com/en-us/library/gg682140.aspx. Luettu: 16.3.2016.

Microsoft 2016. System Center Configuration Manager and Microsoft Intune. Luettavissa: http://download.microsoft.com/download/5/D/B/5DBEBA38-8D5D-4119-B2E8-B8369B74BF43/system_center_configuration_manager_and_microsoft_intune_datasheet.pdf. Luettu: 17.3.2016.

NVD 2016. National Vulnerability Database. National Institute of Standards and Technology. Luettavissa: https://web.nvd.nist.gov/view/vuln/search-advanced. Luettu: 10.3.2016.

Praxiom Research Group Limited 2014. ISO 27000 Infosec Definitions. Luettavissa: http://www.praxiom.com/iso-27000-definitions.htm. Luettu: 28.2.2016.

VAHTI 03 2007. Tietoturvallisuudella tuloksia. Valtiovarainministeriö. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=8c85fe8f-aa4c-4e67-9236-2fee696498a9&groupId=10128&groupId=10229. Luettu: 20.2.2016.

VAHTI 08 2008. Valtionhallinnon tietoturvasanasto. Valtiovarainministeriö. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10128&groupId=10229. Luettu: 17.2.2016.